WHAT'S NEW WHAT'S NEXT @NRB

LA QUINZAINE DE NRB DU 23/11 AU 3/12/2020

Mercredi 02/12

LA JOURNÉE DE LA SÉCURITÉ ET DU DISASTER RECOVERY

NRB
DARING TO COMMIT

WHAT'S NEW WHAT'S NEXT

NRB SOC: "Sécurisez vos opérations lors de changements technologiques radicaux"

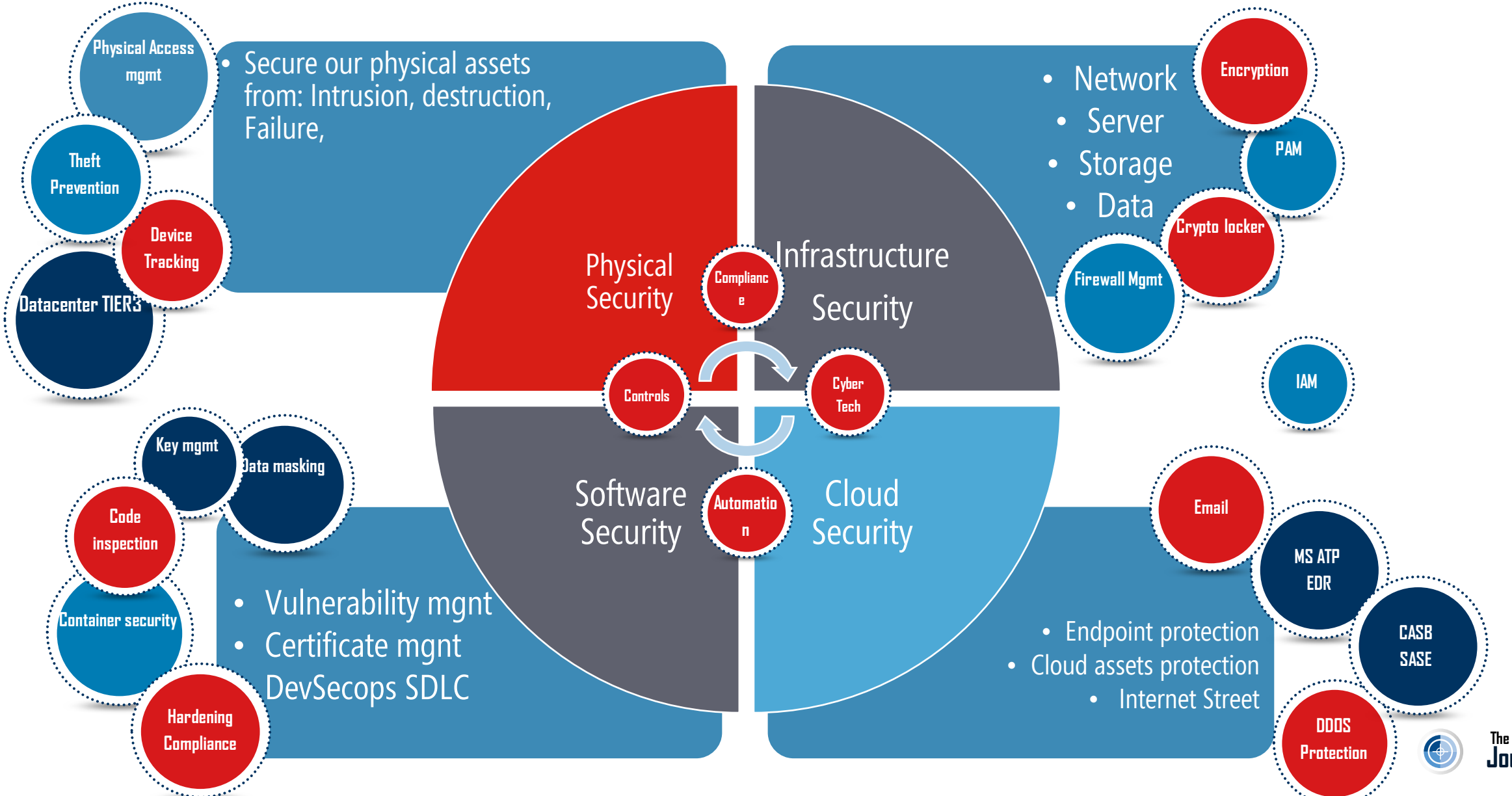
Michaël Boeckx, CTO-CSO NRB

Michel Iwaschko, Security Coordinator NRB

Agenda

- Security Operation Services
- Vulnerability Management Services
- File Crypto Protection Services
- Endpoint Detection and Response (EDR)

Security operations services



Agenda

Security Operation Services

Vulnerability Management Services

Files Crypto Protection Services

Endpoint Detection and Response (EDR)

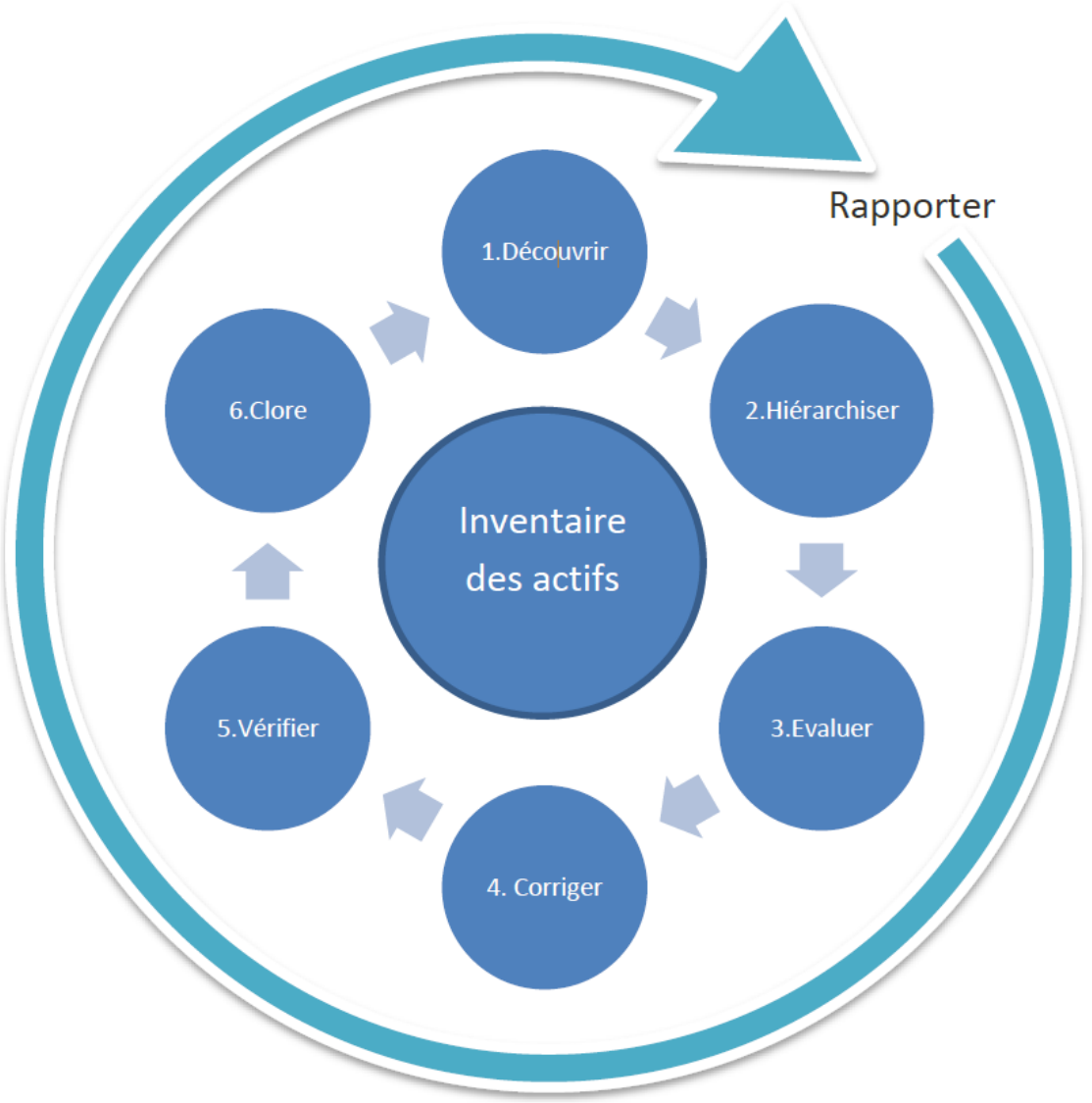
Vulnerability Management Services

- Les vulnérabilités sont inhérentes aux technologies.
- Chaque jour, de nouvelles vulnérabilités sont découvertes et publiées.
- « Vulnerability Management Services» permet :
    - d'analyser,
    - de détecter,
    - d’identifier les problèmes de vulnérabilités.

Vulnerability Management Services

Description des phases du service

1. Découvrir
2. Hiérarchiser
3. Evaluer
4. Corriger
5. Vérifier
6. Clôturer



Agenda

Security Operation Services

Vulnerability Management Services

Files Crypto Protection Services

Endpoint Detection and Response (EDR)

Files Crypto Protection Services

- De plus en plus d'entreprises sont les cibles de ransomwares.
- La restauration à partir de sauvegardes entraîne souvent des pertes de jours de travail.
- Les dommages économiques aux entreprises concernées sont généralement énormes.

File Crypto Protection Services

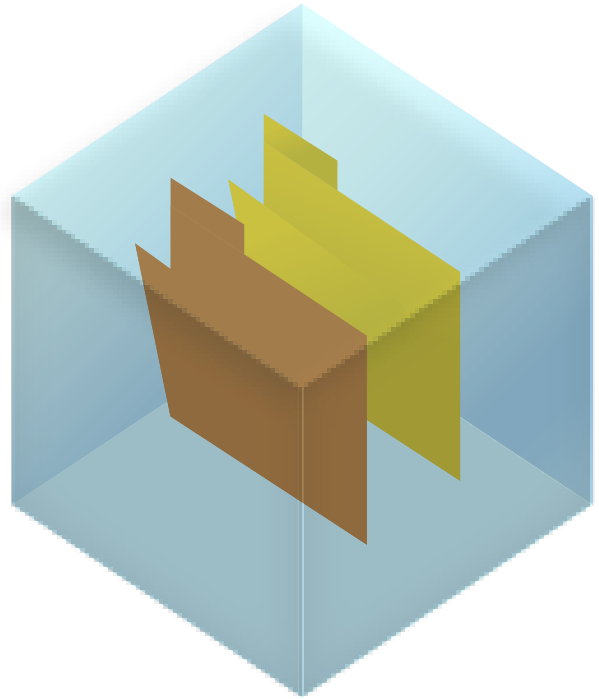
Blocage de l'utilisateur

- Déterminer un comportement inhabituel grâce à l'I.A.
- Connaître l'utilisateur infecté.
- Bloquer l'utilisateur. (Droit d'accès en lecture seul)
- Déclencher la création d'une image des fichiers automatiquement.
- Alerter les équipes de sécurité et opérationnelles.

File Crypto Protection Services

Récupération des fichiers cibles infectés

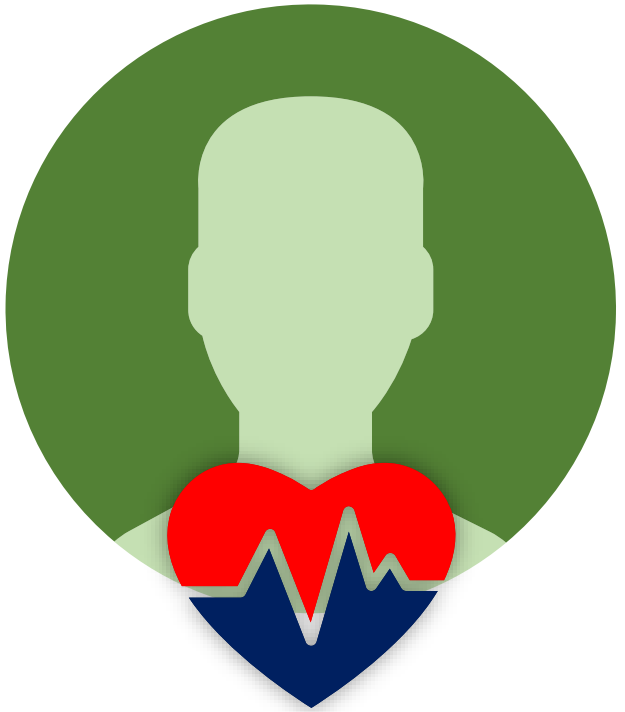
- Identifier les fichiers infectés.
- Permettre la récupération des fichiers infectés.
- Récupération ciblée. (Sans avoir à récupérer l'entièreté d'un disque ou d'un répertoire)



File Crypto Protection Services

Correctif – Remédiation - Audit

- Identifier directement l'utilisateur infecté.
- Rapidité d'action pour l'équipe de sécurité.
- Permet l'audit de l'accès aux fichiers.
    - Qui ?
    - Quoi ?
    - Quand ?



Agenda

Security Operation Services

Vulnerability Management Services

Files Crypto Protection Services

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR)

- Tous les jours des milliers de terminaux sont compromis.
- Les antivirus historiques ne suffisent plus.
- Le manque de corrélation. (On se concentre sur le terminal infecté)
- Ne pas avoir une vue sur l'historique de l'attaque.

Endpoint Detection and Response (EDR)

Détection

- Analyse comportementale grâce à l'I.A.
- Monitore les actions des terminaux.
- Surveille les appels aux registres/mémoires.
- Le suivi dynamique de comportement (DPA)
- Les mouvements latéraux,..

Endpoint Detection and Response (EDR)

Réponse

- Capacités similaires à celles d'un antivirus:
  - Bloquer, supprimer et mettre en quarantaine des fichiers.
- Répondre automatiquement à certaines détections:
  - Isolation d'un terminal, remédiation, recovery, …
- Alerte automatique de l'équipe de Sécurité.

Endpoint Detection and Response (EDR)

Investigation

- Recherche les suites d'actions douteuses.
- Facilite l'investigation des équipes de sécurité.
- Corrélation des actions.
- Remontée dans une plateforme centralisée.
- Historique de l'attaque.
- Création de rapports sur l'état du parc.

What's new?

Les nouveaux services SOC de NRB sont:

- Ransomware Crypto Protection Services
- Endpoint Detection and Response (EDR)
- Vulnerability Management Services
- Certification
- Services SOC 24/7

What's next?

- L' I.A. à l'aide de la sécurité:
  - Les analyses comportementales
  - L'analyse forensique après incident.
- Orchestration des processus et des procédures de réponse aux incidents (Playbooks)
- Corrélation et centralisation des évènements sécurités
- Red Teaming

NRB SOC: "Sécurisez vos opérations lors de changements technologiques radicaux«

Q & R

WHAT'S NEW
WHAT'S NEXT
@NRB

LA QUINZAINE DE NRB DU 23/11 AU 3/12/2020

Marketing@nrb.be
www.nrb.be

NRB
DARING TO COMMIT

WHAT'S NEW WHAT'S NEXT

La consultance cybersécurité : "entre les cadres de conformité et la réalisation"

Vincent Ceriani, Head of Cyber Risk Services NRB

« entre les cadres de conformité et la réalisation »

Agenda
Consultance CyberSécurité

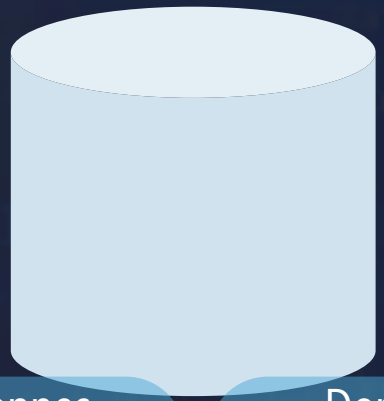
- GDPR – DPO
- ISO27K – Mise en conformité
- Identity and Access Management

« entre les cadres de conformité et la réalisation »

Agenda
Consultance CyberSécurité

- GDPR – DPO
- ISO27K – Mise en conformité
- Identity and Access Management

DIFFÉRENTES LÉGISLATIONS DEMANDENT DES RÈGLES POUR LA GESTION DES DONNÉES À CARACTÈRE PERSONNEL



Personnes concernées

Données à caractère personnel

RGDP

Lois nationales

Directive NIS

Lois sectoriels

Collecter

Sauvegarder

Utiliser

Traitement des données

NRB
DARING TO COMMIT

APPROCHE NRB À LA MISE EN CONFORMITÉ RGDP

Phase 1 — **Étude préliminaire (Découverte)**

- Cartographie des données et traitements
- Analyse des risques 'vie privée'
- Écarts de conformité
- Plan d'action

Phase 2 — **Mise en conformité**

- Politique 'vie privée'
- Procédures liées aux droits des personnes concernées
- Informer les personnes concernées
- Gérer les violations
- Gérer les contracts (et sous-traitants)
- Sensibiliser le personnel

Annuel — **Maintenance Périodique**

- Audit annuel
- Analyse des évolutions
- Actualiser le registre de traitements
- Actualiser l'action plan

Ad Hoc — **Support DPO**

- Traitement des demandes des personnes concernées
- Formation / Q&R
- Assistance DPO et recommendations
- Collaboration avec les autorités
- Gestion des violations DàCP
- Suivi du plan d'action

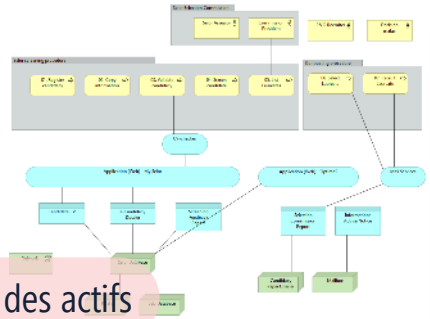
NRB
DARING TO COMMIT

PHASE 1 – ÉTUDE PRÉLIMINAIRE (DÉCOUVERTE)

Phase 1

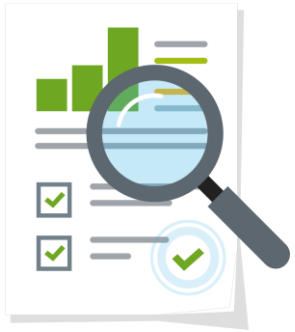
Découverte

NRB planifie une analyse approfondie et fournit des recommandations basées sur une analyse des risques



Cartographie des actifs

Cartographie données et traitements



Écarts de conformité

Fiche de traitement

Analyse des risques

Plan d'action

Call to action!

APPROCHE NRB À LA MISE EN CONFORMITÉ RGDP

Phase 1 — **Étude préliminaire (Découverte)**

- Cartographie des données et traitements
- Analyse des risques 'vie privée'
- Écarts de conformité
- Plan d'action

Phase 2 — **Mise en conformité**

- Politique 'vie privée'
- Procédures liées aux droits des personnes concernées
- Informer les personnes concernées
- Gérer les violations
- Gérer les contracts (et sous-traitants)
- Sensibiliser le personnel

Annuel — **Maintenance Périodique**

- Audit annuel
- Analyse des évolutions
- Actualiser le registre de traitements
- Actualiser l'action plan

Ad Hoc — **Support DPO**

- Traitement des demandes des personnes concernées
- Formation / Q&R
- Assistance DPO et recommendations
- Collaboration avec les autorités
- Gestion des violations DàCP
- Suivi du plan d'action

NRB
DARING TO COMMIT

PHASE 2 – MISE EN CONFORMITÉ

Phase 2

Mise en conformité

NRB apporte des livrables standards, qui seront personnalisés sous forme de workshop

- Politique RGPD
- Procédures liées aux droits des personnes concernées
- Informer les personnes concernées
- Gestion des violations, incidents de sécurité
- Gestion des contrats
- Contrôles et Mesures de sécurité

Modèles standard

NRB-input

Personnalisation

Workshop

Livrables personnalisés

NRB-output

Personnalisation

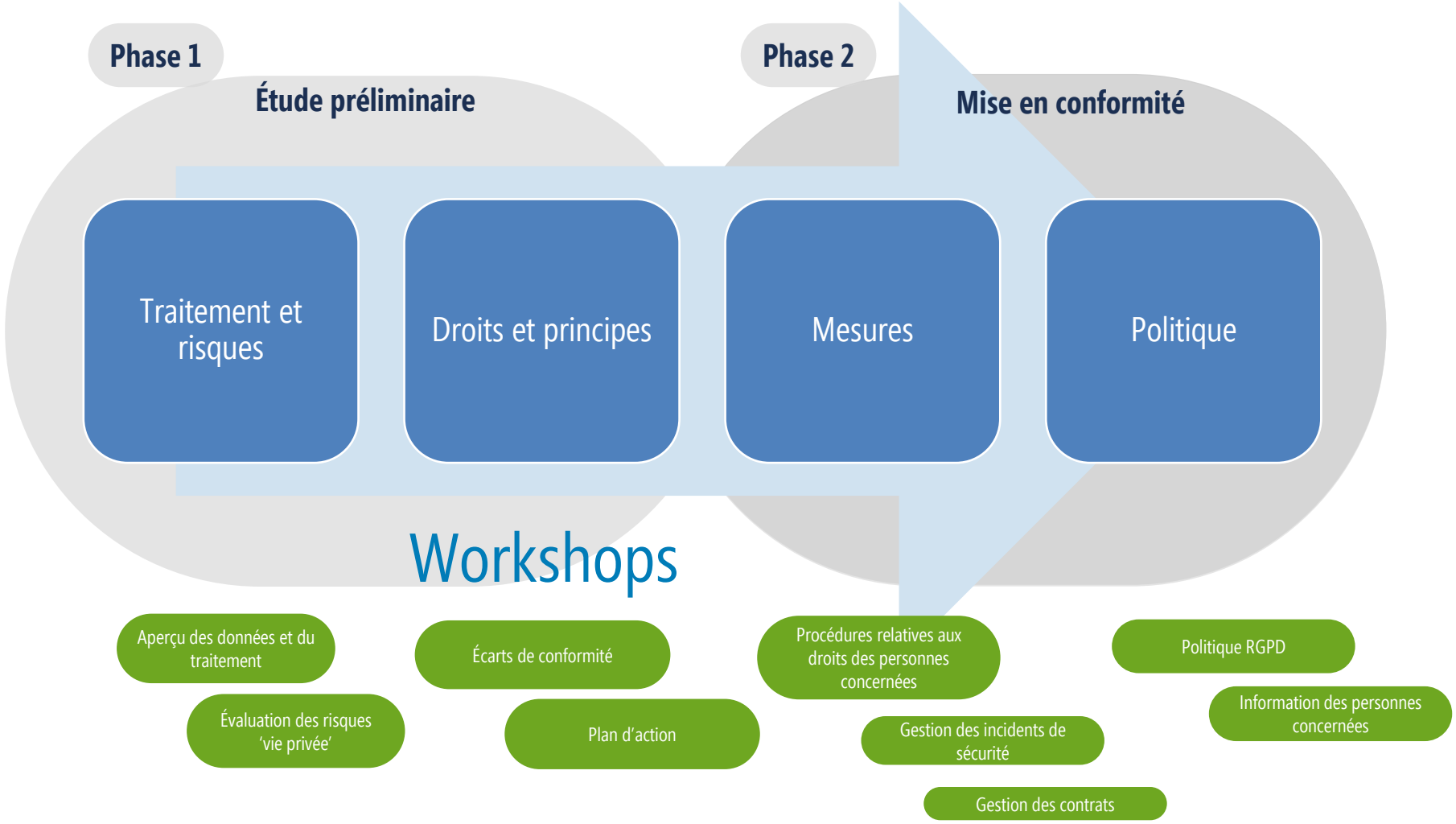
Validation des livrables par le DPO

FINAL

GDPR MASTER CLASS – Mise en pratique

GDPR Master Class

À travers des ateliers, NRB réalise une sensibilisation et formation par la mise en situation réelle du travail aux personnes clés dans votre organisation



APPROCHE NRB À LA MISE EN CONFORMITÉ RGDP

Phase 1 — **Étude préliminaire (Découverte)**

- Cartographie des données et traitements
- Analyse des risques 'vie privée'
- Écarts de conformité
- Plan d'action

Phase 2 — **Mise en conformité**

- Politique 'vie privée'
- Procédures liées aux droits des personnes concernées
- Informer les personnes concernées
- Gérer les violations
- Gérer les contracts (et sous-traitants)
- Sensibiliser le personnel

Annuel — **Maintenance Périodique**

- Audit annuel
- Analyse des évolutions
- Actualiser le registre de traitements
- Actualiser l'action plan

Ad Hoc — **Support DPO**

- Traitement des demandes des personnes concernées
- Formation / Q&R
- Assistance DPO et recommendations
- Collaboration avec les autorités
- Gestion des violations DàCP
- Suivi du plan d'action

NRB
DARING TO COMMIT

RGPD VA DE PAIR AVEC LA SÉCURITÉ DE L'INFORMATION

Phase 1 — **Étude préliminaire (Découverte)**

- Cartographie des données et traitements
- Analyse des risques 'vie privée'
- Écarts de conformité
- Plan d'action

- Cartographie des actifs
- Analyse des risques 'sécurité de l'information'
- Analyse de maturité
- Plan de sécurité

Phase 2 — **Mise en conformité**

- Politique 'vie privée'
- Procédures liées aux droits des personnes concernées
- Informer les personnes concernées
- Gérer les violations
- Gérer les contrats (et sous-traitants)
- Sensibiliser le personnel

- Politique de sécurité
- Mesures de sécurité
- Registrer et consigner
- Gérer les incidents
- Sensibiliser le personnel

NRB
DARING TO COMMIT

NRB VOUS AIDE À GÉRER VOS DONNÉES CONFORMÉMENT À LA RÉGLEMENTATION DANS LE DOMAINE DE LA VIE PRIVÉE

CADRE RÉGLEMENTAIRE 'VIE PRIVÉE'

PIMS

- DPO
- Politique vie privée
- Principes
- Droits
- Mesures
- Registres RGPD
- Violations

bsi. ISO/IEC 27701 Privacy Information Management

COMPOSANTS POUR LA CONFORMITÉ

- Modèles pour créer une politique 'vie privée'
- Procédures relatives aux droits des personnes concernées
- Techniques pour informer les personnes concernées
- Processus pour gérer les violations, incidents de sécurité
- Gérer les contrats
- Sensibiliser le personnel

NRB
DARING TO COMMIT

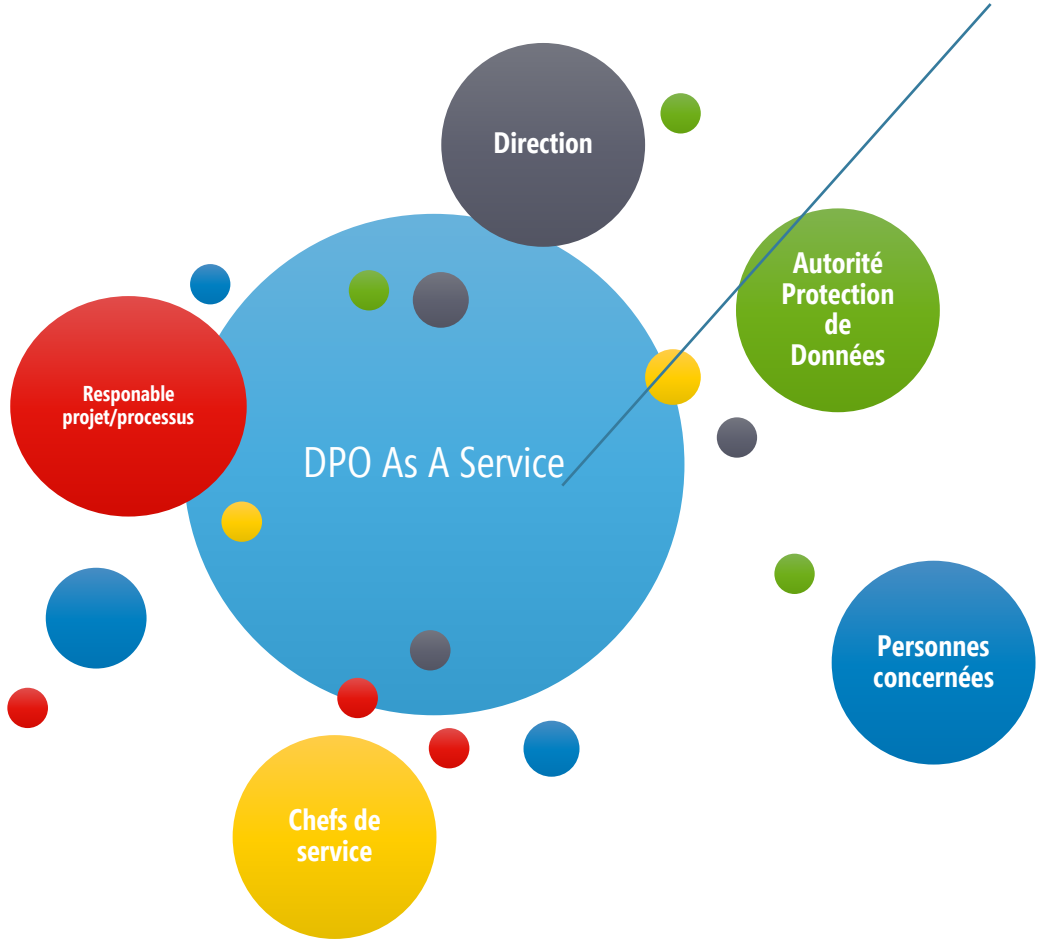
MISSION DPO – POINT DE CONTACT RGPD POUR VOTRE ORGANISATION

Data Protection Officer

Centre de Service

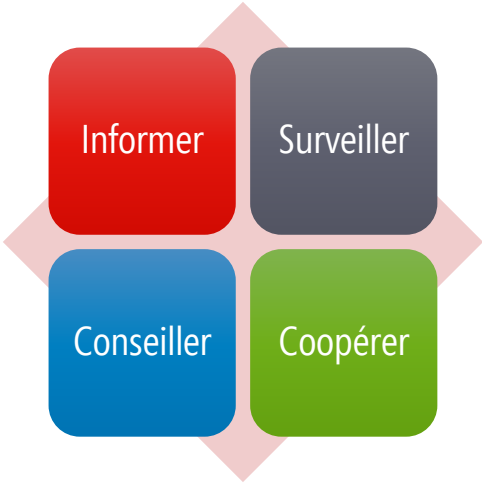
Activités

NRB organise le rôle de DPO comme un centre de service neutre et compétent auprès de votre organisation



Activités

Publication des articles RGPD sur intranet
Sensibilisation RGPD lors d'une réunion d'équipe
Réponses aux demandes
Recommendations pour réaliser vos projets
Réunion de travail pour réaliser le registre RGPD
Rédaction des demandes d'accès aux sources authentiques
Rédaction des contrats de sous-traitance
Avis RGPD lors d'une procédure de marché public
…



NRB
DARING TO COMMIT

NRB APPLIQUE LES BONNES PRATIQUES

cases.lu
Cyberworld Awareness and Security Enhancement Services
LUXEMBOURG

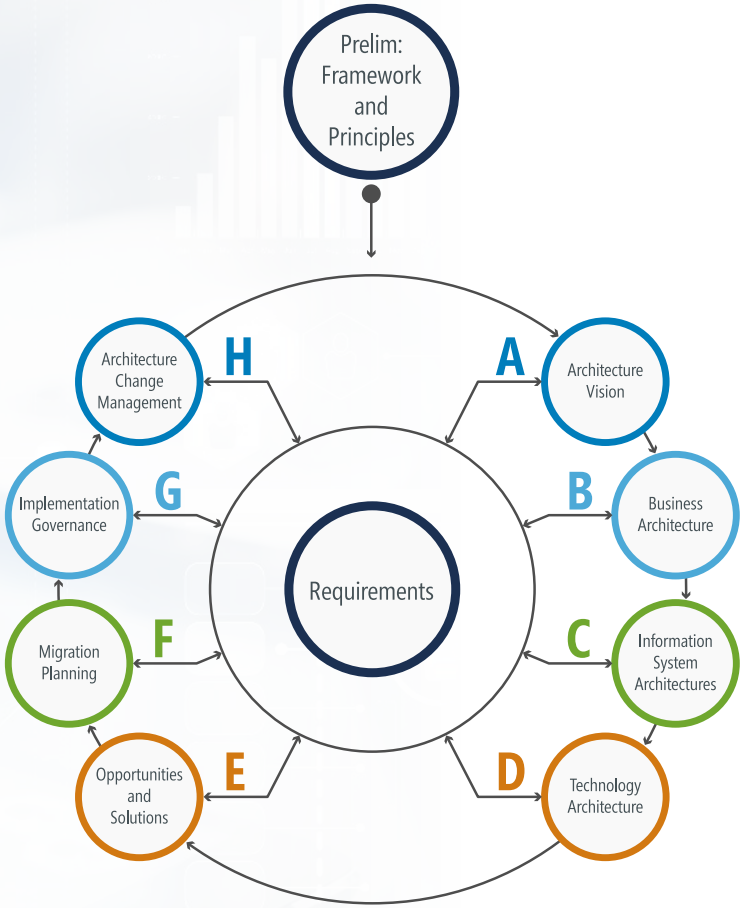
CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Archi
archimate modelling

EGERIE
PRIVACYMANAGER

bsi. ISO/IEC 27701 Privacy Information Management

edpb
European Data Protection Board



NRB
DARING TO COMMIT

« entre les cadres de conformité et la réalisation »

Agenda
Consultance CyberSécurité

GDPR – DPO

ISO27K – Mise en conformité

Identity and Access Management

NOUVELLES TECHNIQUES DE CYBER CRIME CRÉENT DES NOUVEAUX DÉFIS POUR LA SÉCURITÉ DE L'INFORMATION

HACKER

Variété des données à protéger

- Identification
- Contacts
- Financier
- Composition familiale
- Compte bancaire
- Paiements
- Location
- Intérêts
- Possessions
- Dossier médical
- cv
- Carrière

NRB
DARING TO COMMIT

NOTRE APPROCHE EN SECURITE D'INFORMATION

Phase 1 — **Etude préliminaire**

- Cartographie des actifs
- Analyse de risques
- Analyse de maturité
- Plan de sécurité

Phase 2 — **Implémentation SMSI**

- Politiques de sécurité
- Mesures de sécurité
- Registres et inventaires des actifs
- Gestion des incidents
- Sensibilisation du personnel

Annuel — **Maintenance périodique**

- Actualiser la cartograhie
- Actualiser les risques
- Actualiser le plan de sécurité
- Gestion administrative

Ad Hoc — **Support**

- Traitement des incidents
- Training/Formation
- Workshop relatif à un sujet spécifique
- Suivi du plan de sécurité
- Rapport annuel sur base d'un audit

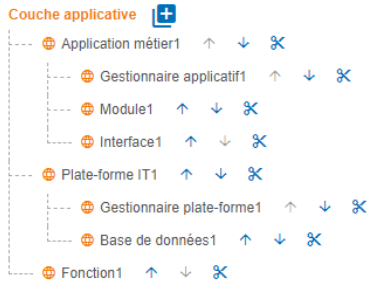
NRB
DARING TO COMMIT

PHASE 1 – ÉTUDE PRÉLIMINAIRE

Phase 1

Étude préliminaire

NRB réalise une analyse approfondie et fournit des recommandations basées sur une analyse des risques



cases.lu
Cyberworld Awareness and Security Enhancement Services
LUXEMBOURG

Cartographie des actifs

Analyse des risques

Écarts par rapport aux normes

Plan d'action

Plan de sécurité

NRB
DARING TO COMMIT

PHASE 1 – PLAN DE SÉCURITÉ

Phase 1

Étude préliminaire

Plan d'action

Le plan de sécurité est livré sous forme de document accompagné de graphiques qui facilitent la prise de décision

cases.lu
Secure. Innovate. Lead.

Rapport Final

Sécurité de l'information - MONARC

Informations générales

Version:	5
État document:	Final
Classification:	
Société:	
Nom du document:	Rapport Final
Date:	07/05/2020
Consultant(e) sécurité:	
Représentant(e) client:	

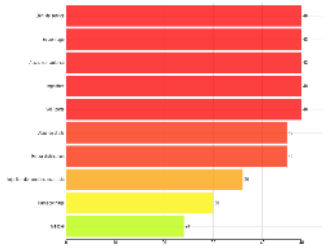
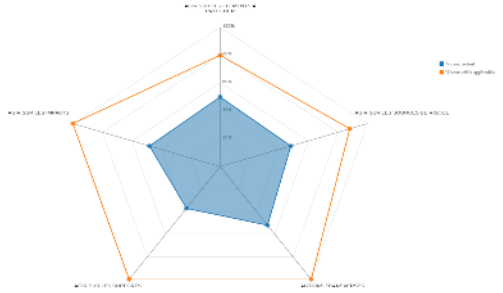
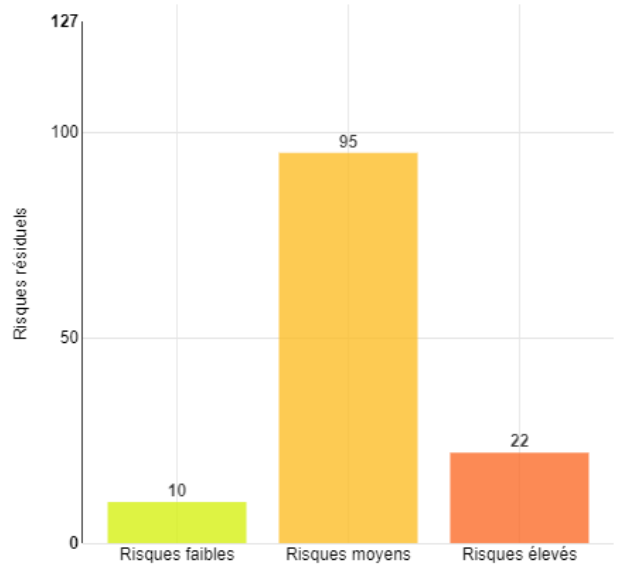


Table des matières





NOTRE APPROCHE EN SECURITE D'INFORMATION

Phase 1 — **Etude préliminaire**

- Cartographie des actifs
- Analyse de risques
- Analyse de maturité
- Plan de sécurité

Phase 2 — **Implémentation SMSI**

- Politiques de sécurité
- Mesures de sécurité
- Registres et inventaires des actifs
- Gestion des incidents
- Sensibilisation du personnel

Annuel — **Maintenance périodique**

- Actualiser la cartograhie
- Actualiser les risques
- Actualiser le plan de sécurité
- Gestion administrative

Ad Hoc — **Support**

- Traitement des incidents
- Training/Formation
- Workshop relatif à un sujet spécifique
- Suivi du plan de sécurité
- Rapport annuel sur base d'un audit

NRB
DARING TO COMMIT

NRB AIDE À METTRE EN PLACE UN SYSTÈME DE GESTION DE LA SÉCURITÉ DE L'INFORMATION (ISMS) PERSONNALISÉ

CADRE TECHNIQUE SÉCURITÉ DE L'INFORMATION

ISMS

- CISO
- Politique de sécurité
- Tester les principes
- Domaine de la sécurité de l'information
- Mesures
- Cartographie
- Incidents

bsi. ISO/IEC 27001 Information Security Management

CONFORMITÉ

- Politique de sécurité
- Mesures de sécurité
- Registres et fichier log
- Gestion des incidents
- Sensibilisation du personnel

NRB
DARING TO COMMIT

« entre les cadres de conformité et la réalisation »

Agenda
Consultance CyberSécurité

- GDPR – DPO
- ISO27K – Mise en conformité
- **Identity and Access Management**

DÉFINITION

IDENTITY AND ACCESS MANAGEMENT (IAM)

- **Processus** qui permet aux BONNES PERSONNES d'accéder aux BONNES RESSOURCES au BON MOMENT pour les BONNES RAISONS.
- Ce **processus** doit être accompagné d'une **gouvernance**.
- Pour le **mettre en place** et le **faire vivre**, il a besoin d'outils pour
    - CENTRALISER,
    - AUTOMATISER,
    - FACILITER.

IAM: POURQUOI ?

- Pour maîtriser les risques Sécurité en gérant les accès
- Pour être compliant aux normes ISO27K et GDPR
- Pour augmenter la productivité
- Pour faciliter/automatiser la gestion des comptes
- Pour diminuer les encodages manuels et donc les erreurs potentielles
- Pour renforcer la maîtrise des accès business et administrateurs (internes et externes)

IAM - Définition

IDENTITY AND ACCESS MANAGEMENT FRAMEWORK (IAMF)

Identity Governance (GRC)

Identity Management (IM)

- Generate
- Register
- Distribute/bind
- Proof
- Store/update
- Reset
- Expire/renew
- Recover
- Revoke/dispos

Access Management (AM) & Web AM Single Sign-On (SSO)

- Request & approve
- Provision & de-provision
- Enforce
- Review & certify
- Reconcile
- Report & audit

Directories

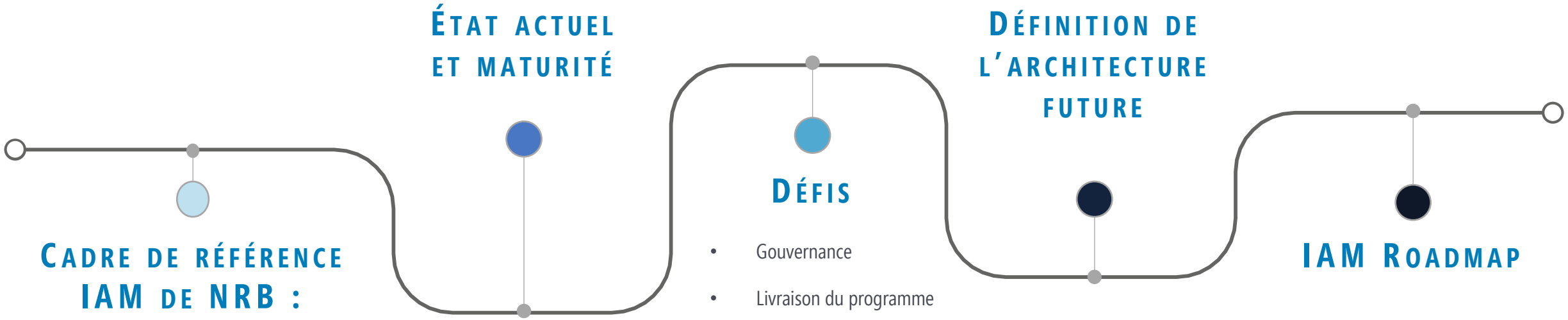
- HR Information
- Hierarchy information
- Roles & rules
- IAM Warehouse

Applications and Systems

PRIVILEGED ACCOUNT SECURITY

NRB
DARING TO COMMIT

APPROCHE



CADRE DE RÉFÉRENCE IAM DE NRB :

- Gouvernance
- Identité et Identification (‘Credential’)
- L’accès
- Sources ‘authoritative’ (faisant autorité)
- Administration et gestion

ÉTAT ACTUEL ET MATURITÉ

DÉFIS

- Gouvernance
- Livraison du programme
- Conformité
- Cycle de vie de l’identité
- Contrôle accès
- Opérations

DÉFINITION DE L’ARCHITECTURE FUTURE

IAM ROADMAP

QUICK WINS

APPORTER AU BUSINESS LES AVANTAGES DE LA SOLUTION

- Analyser les besoins et les prioritiser
- Identifier la ou les solutions adaptées aux besoins
- Viser des objectifs concrets, réalistes
- Mettre rapidement en production les premiers résultats
- Adapter les procédures et la gouvernance
- Elargir le périmètre progressivement

COMMENT RATER VOTRE PROJET IAM ?

LES PIÈGES À ÉVITER

- Tout vouloir, tout de suite
- Bâcler le choix de la solution
- Penser qu'une simple installation du produit suffit
- Abuser du développement spécifique
- Oublier qu'il y a une vie après la production

What's new?

- Gouvernance
- DPO as a Service
- CISO as a Service
- IAM / CIAM
- Sécurité Opérationnelle

What's next?

- Amélioration continue des processus
- Gouvernance -> SecOps -> Opérations

La consultance cybersécurité : "entre les cadres de conformité et la réalisation"

Q & R

WHAT'S NEW
WHAT'S NEXT
@NRB

LA QUINZAINE DE NRB DU 23/11 AU 3/12/2020

Marketing@nrb.be
www.nrb.be

NRB
DARING TO COMMIT

WHAT'S NEW WHAT'S NEXT

Cloud security: "Système back end et protection de terminaux dans un monde de hyperscalers"

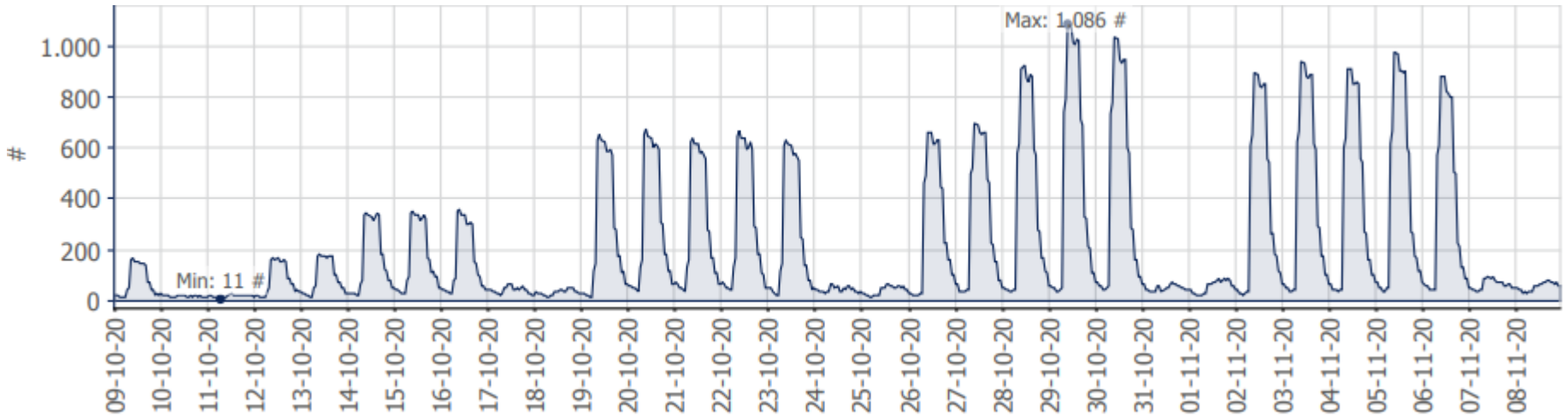
Simon Melotte, Cloud Product ManagerNRB

Agenda

- Covid-19 #newnormal
- VPN Client à Site
- Proxy in the cloud
- Cloud Access Security Broker (CASB)
- Secure Access Service Edge (SASE)

#newnormal

Nous sommes passés de 15 à 20 % à 80-90 % de télétravail.



45%

Des employeurs demandent à leurs employés d’utiliser leurs équipements personnels afin de travailler à distance.

Source: research commissioned by Microsoft Ireland

30%

Des travailleurs utilisent leur compte email personnel à des fins professionnels.

Source: research commissioned by Microsoft Ireland

43%

Des travailleurs accèdent à des documents professionnels sans restrictions quand ils travaillent à domicile.

Source: research commissioned by Microsoft Ireland

50%

Des noms de domaines liés au Covid-19 pourraient être liés à des logiciels malveillants.

Source: research commissioned by Microsoft Ireland

26%

Des personnes travaillant à distance ont subi une cyber attaque.

Source: research commissioned by Microsoft Ireland

En 2019

13 milliards d’emails ont été bloqués et 1 milliard de sites ont été créés dans le but de voler des identifiants.

Source: research commissioned by Microsoft Ireland

Agenda

Covid-19 #newnormal

VPN Client à Site

Proxy in the cloud

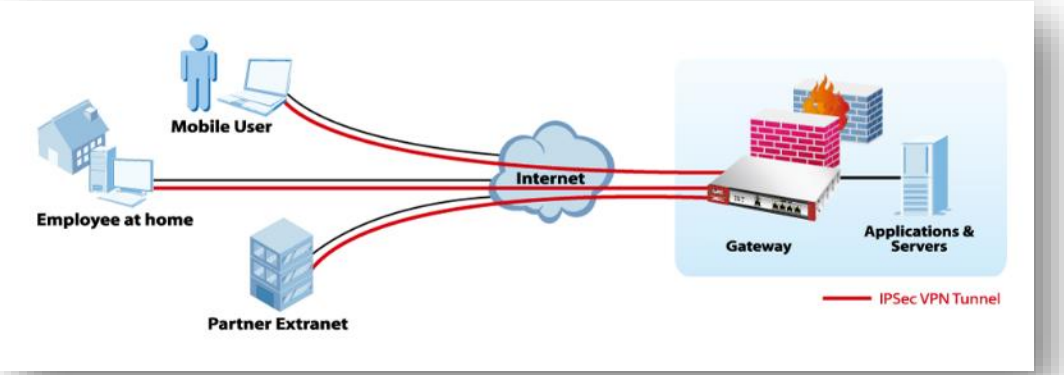
Cloud Access Security Broker (CASB)

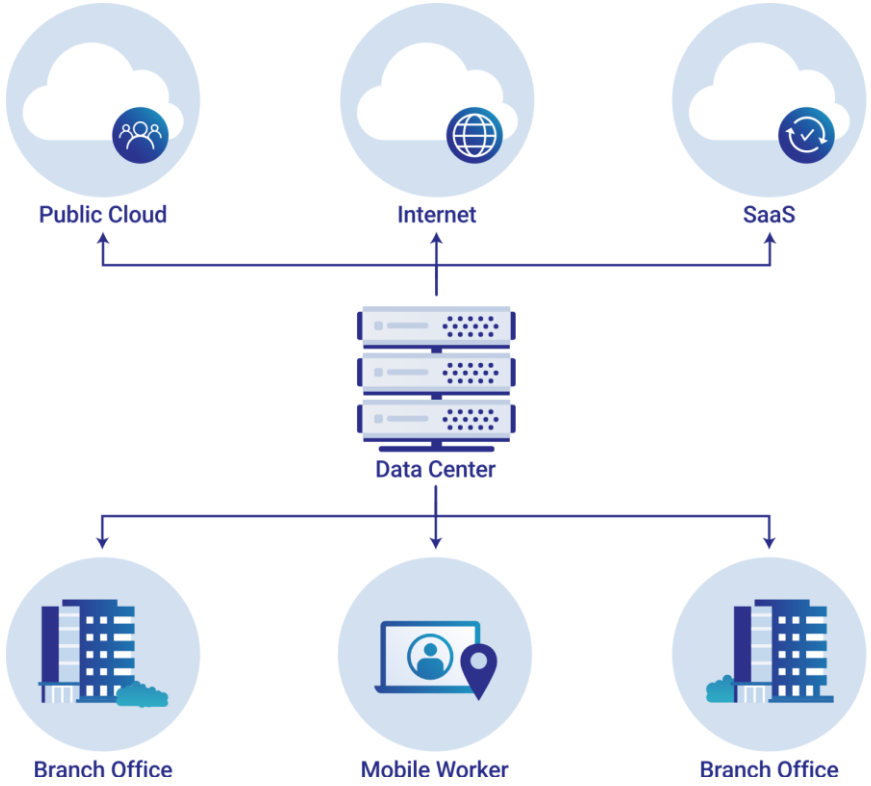
Secure Access Service Edge (SASE)

Comment sécuriser ?

VPN Client-to-Site

- Infrastructure traditionnelle en étoile
- Articuler autour d'un datacenter





Agenda

Covid-19 #newnormal

VPN Client à Site

Proxy in the cloud

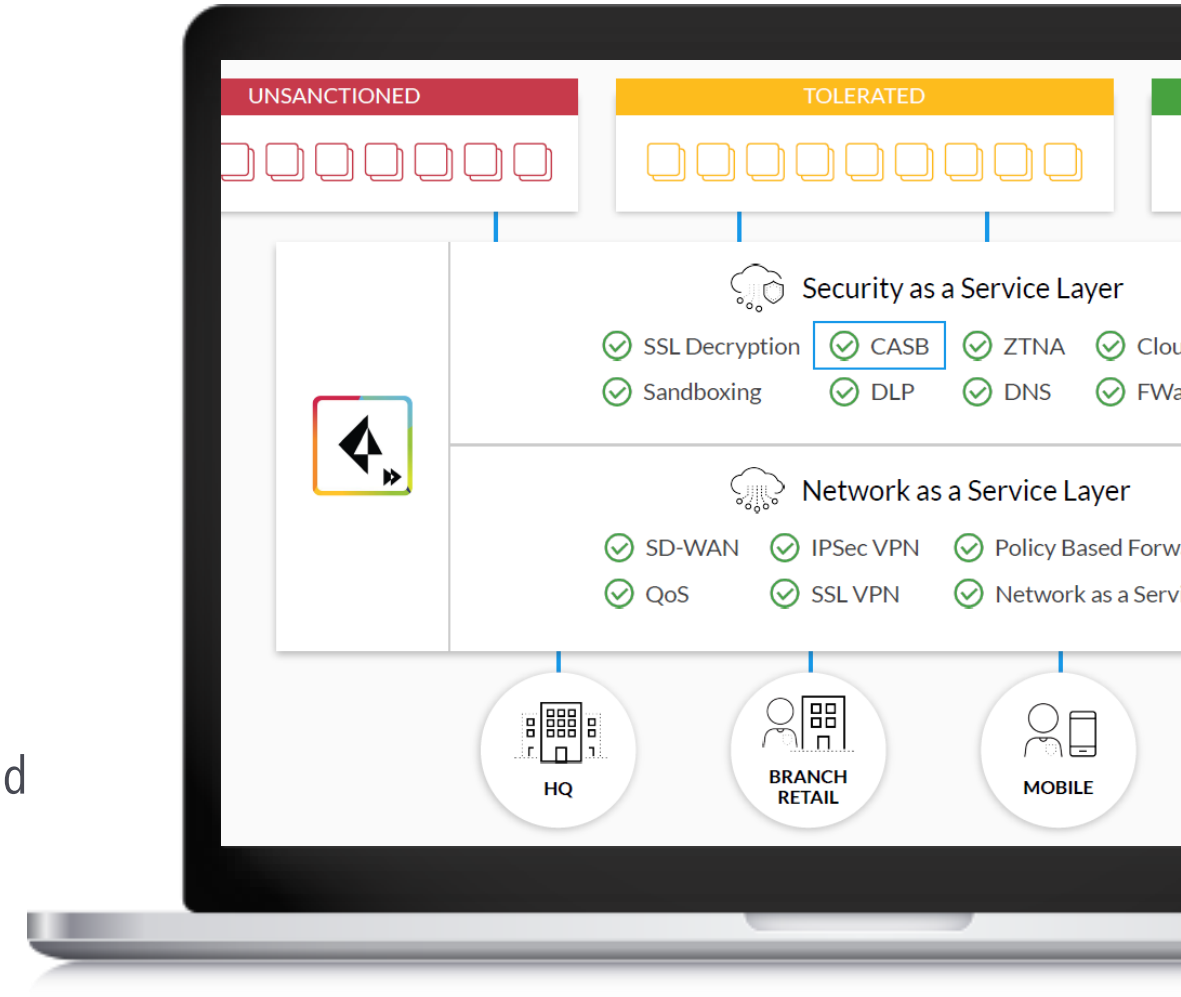
Cloud Access Security Broker (CASB)

Secure Access Service Edge (SASE)

Comment sécuriser ?

Proxy in the cloud

- Sécuriser les utilisateurs distants
- Identification des utilisateurs
- Filtrage d'URL
- Décryption SSL
- Sandboxing
- Offload du trafic vers le datacenter pour les applications cloud



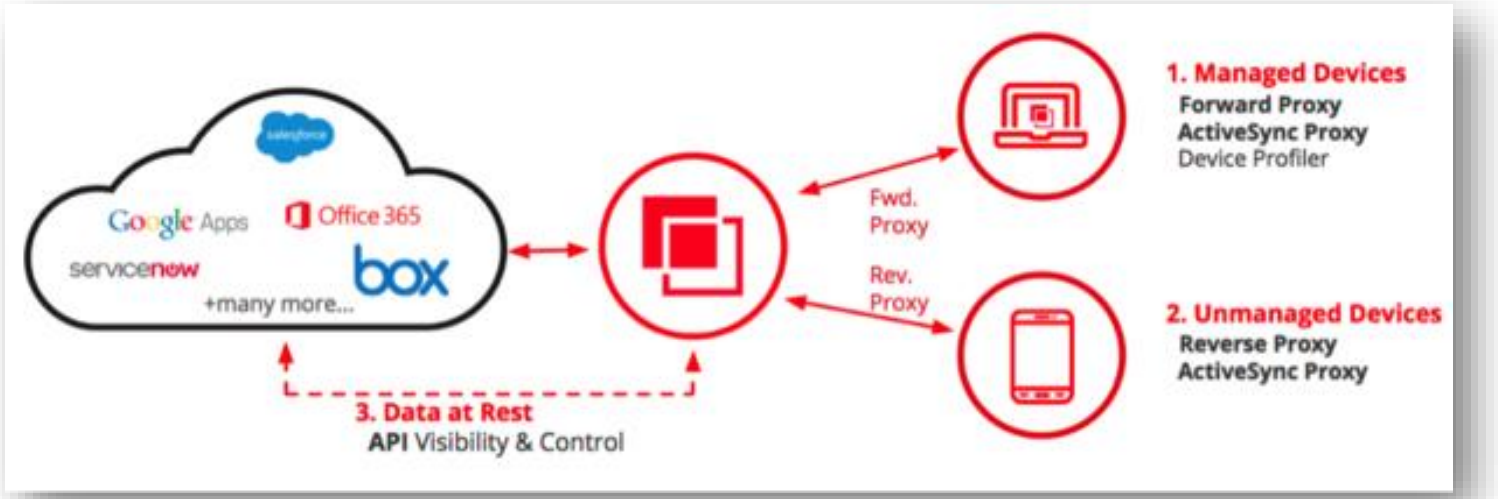
Agenda

- Covid-19 #newnormal
- VPN Client à Site
- Proxy in the cloud
- **Cloud Access Security Broker**
- Secure Access Service Edge (SASE)

Comment sécuriser ?

Cloud Access Security Brokers (CASB)

- Protège les applications cloud
- Gestion des identités
- Contrôle d'accès
- Identification Shadow IT
- Contrôle via API
- Threat Protection
- Data Protection (DLP)



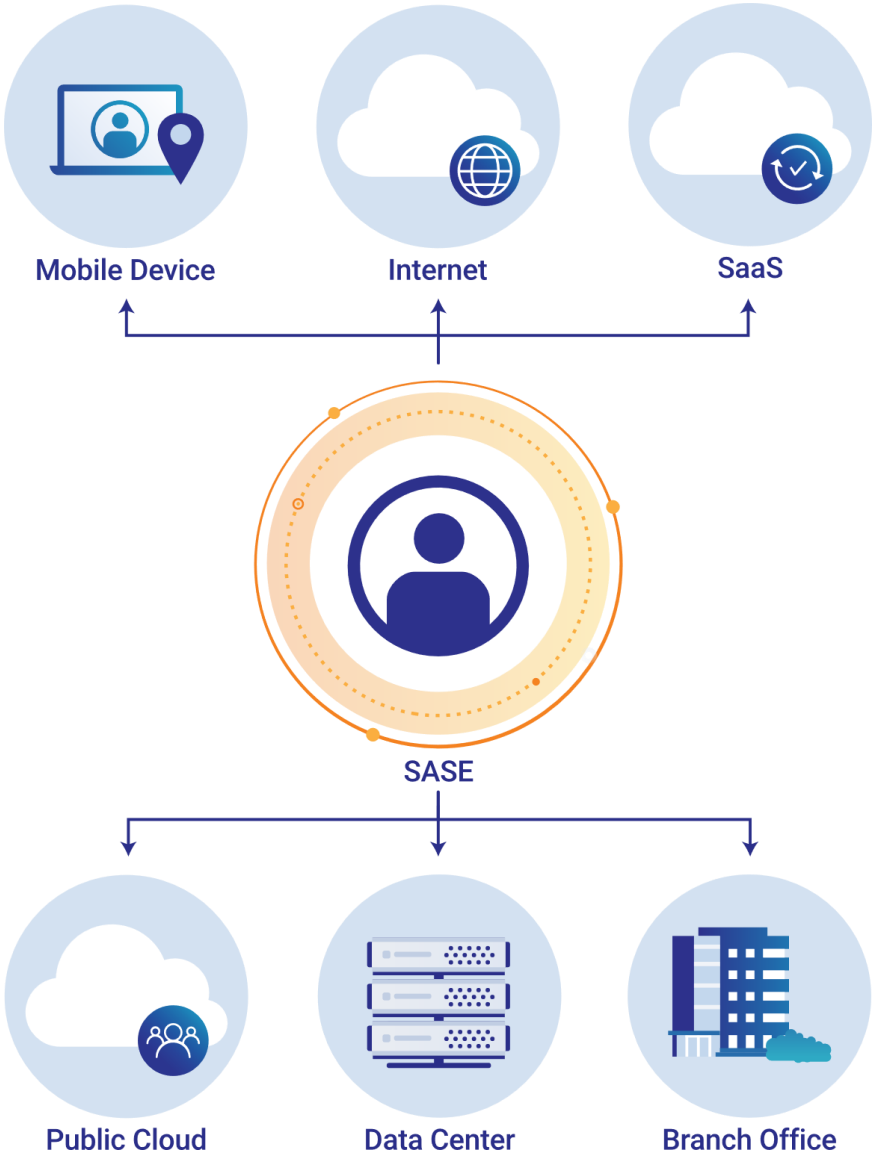
Agenda

- Covid-19 #newnormal
- VPN Client à Site
- Proxy in the cloud
- Cloud Access Security Broker (CASB)
- Secure Access Service Edge

Comment sécuriser ?

Secure Access Service Edge (SASE)

- Solution “all-in-one”
- Fournit les mêmes services que le CASB avec les fonctionnalités supplémentaires suivantes:
    - Firewall en tant que service (next-gen firewall)
        - Filtrage d’URL
        - Protection contre les intrusions
    - Passerelles Internet sécurisées
        - Filtrent les contenus indésirables du trafic web
        - luttent contre la perte de données
    - Un accès Zero Trust au réseau
    - SD-WAN pour interconnecter utilisateurs, bureaux, datacenters et application cloud.



What's new?

- Forte augmentation pour le télétravail
- Nouvelles techniques pour attaquer

What's next?

- Utiliser les technologies clouds afin de pouvoir utiliser l'élasticité qu'ils fournissent
- Faire évoluer nos offres digitales
- Former les personnes
- Utiliser des alternatives aux mots de passe (empreinte digitale ou reconnaissance faciale)


WHAT'S NEW
WHAT'S NEXT
@NRB
Cloud security: "Système back end et protection de terminaux dans un monde de hyperscalers"
Q & R

WHAT'S NEW
WHAT'S NEXT
@NRB

LA QUINZAINE DE NRB DU 23/11 AU 3/12/2020

Marketing@nrb.be
www.nrb.be

NRB

DARING TO COMMIT

WHAT'S NEW WHAT'S NEXT

Disaster Recovery

Patrick Blazy, Disaster Recovery Manager NRB

WHAT'S NEW

LA GENÈSE DES PLANS DR

Analyse de Risque

- Identifier les risques,
- Qualifier leur probabilité d'occurrence,
- Qualifier leur impact
- En déduire leur criticité/gravité

Mitigations:
- Architecture IT
- Tests
- Multi sites
- Assurances
- Audits…

Risques résiduels

Business Impact Analysis

- Evaluer l'impact de la disparition d'activités métiers critiques
- En déduire un délai d'interruption maximum admissible au-delà duquel la survie de l'entreprise est menacée

DMIA :
Délais Maximum d'Interruption Admissible

PDMA :
(=RPO)
Perte de Données Maximale Admissible

Scénarios de crise

Scénario de crise « X »

Plans BCP

Plan BCP « X »

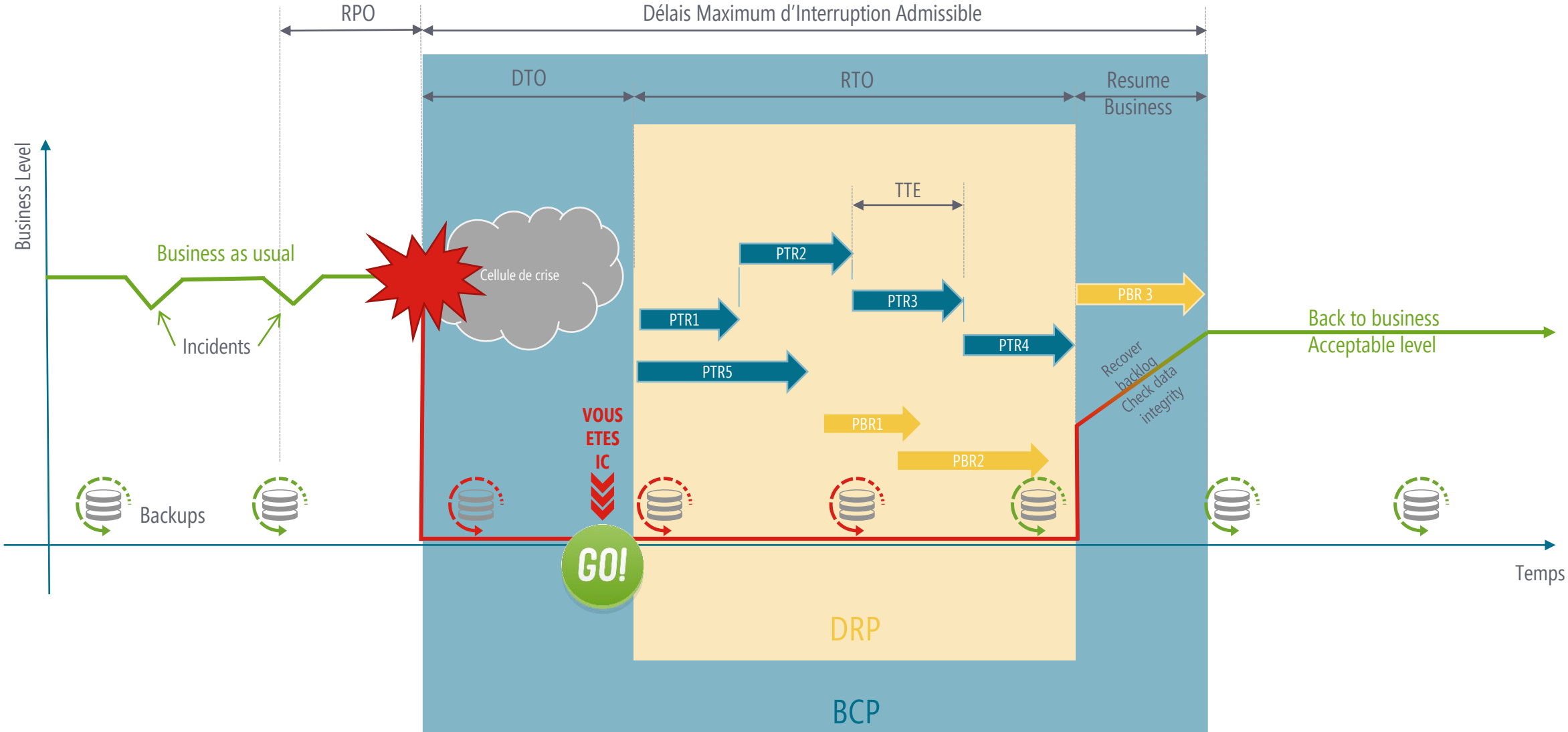
Rétablissement services métiers

Plans DRP

Plan DRP « X »

Rétablissement services IT

LE SÉQUENCEMENT D'UN DÉSASTRE



NRB
DARING TO COMMIT

UNE MÉTHODOLOGIE

- Business Continuity versus Disaster Recovery
- Rôles équipe DR versus équipes techniques
- La documentation et ses révisions
- Le séquencement d'un plan DR
- Bascules techniques versus Tests DR

BUSINESS CONTINUITY VS DISASTER RECOVERY ?

Une frontière pas toujours claire pour tout le monde

BC : HUMAINS, OUTILS ET BUSINESS

Le **Business**

- Gestion de crise
- Les personnes impliquées
- Un espace de travail
- Les outils

DR : INFRASTRUCTURE IT

Les **Infrastructures**

- Comment rétablir
- Qui exécute
- Dans quel ordre
- Outils métier nécessaires

QUI FAIT QUOI ?

Une frontière pas toujours claire pour tout le monde

DR TEAM

- La **méthodologie**
- La consolidation des informations
- Le suivi de la rédaction des plans
- L'organisation des tests DR

TECHNICAL TEAM

- L'identification des infrastructures
- Rédaction et maintenance des PTR
- La réalisation des tests

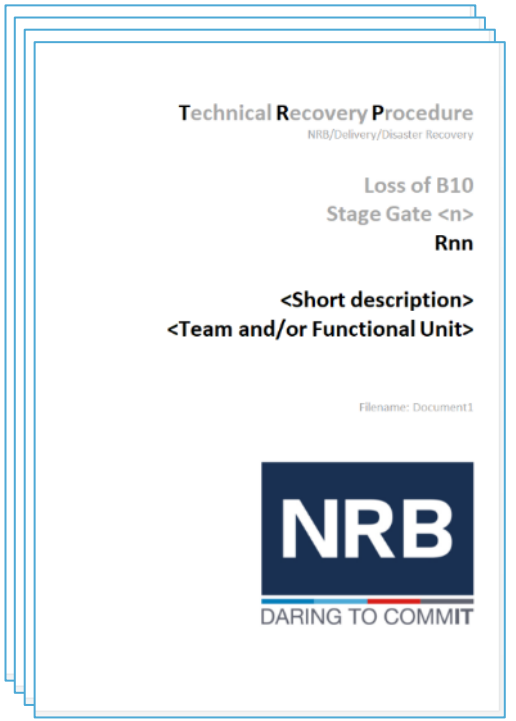
PROCÉDURES TECHNIQUES DE REPRISE (PTR)

TECHNICAL RECOVERY PROCEDURES (TRP)

- Décrit une suite d'actions exécutées **séquentiellement**,

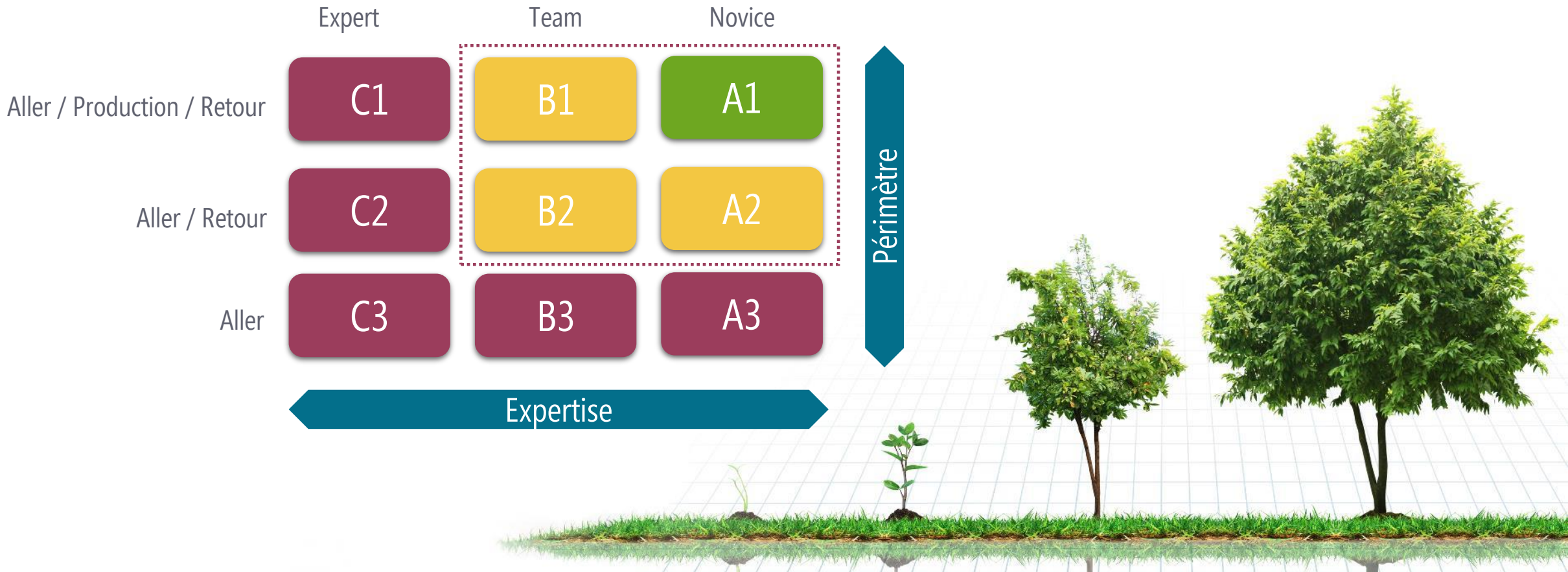
  par la **même équipe** sur un ensemble **cohérent** d'infrastructures

  - Si les actions ne sont pas séquentielles ► PTR supplémentaires
  - Un ensemble de PTR forment une recette (groupement « logique »)

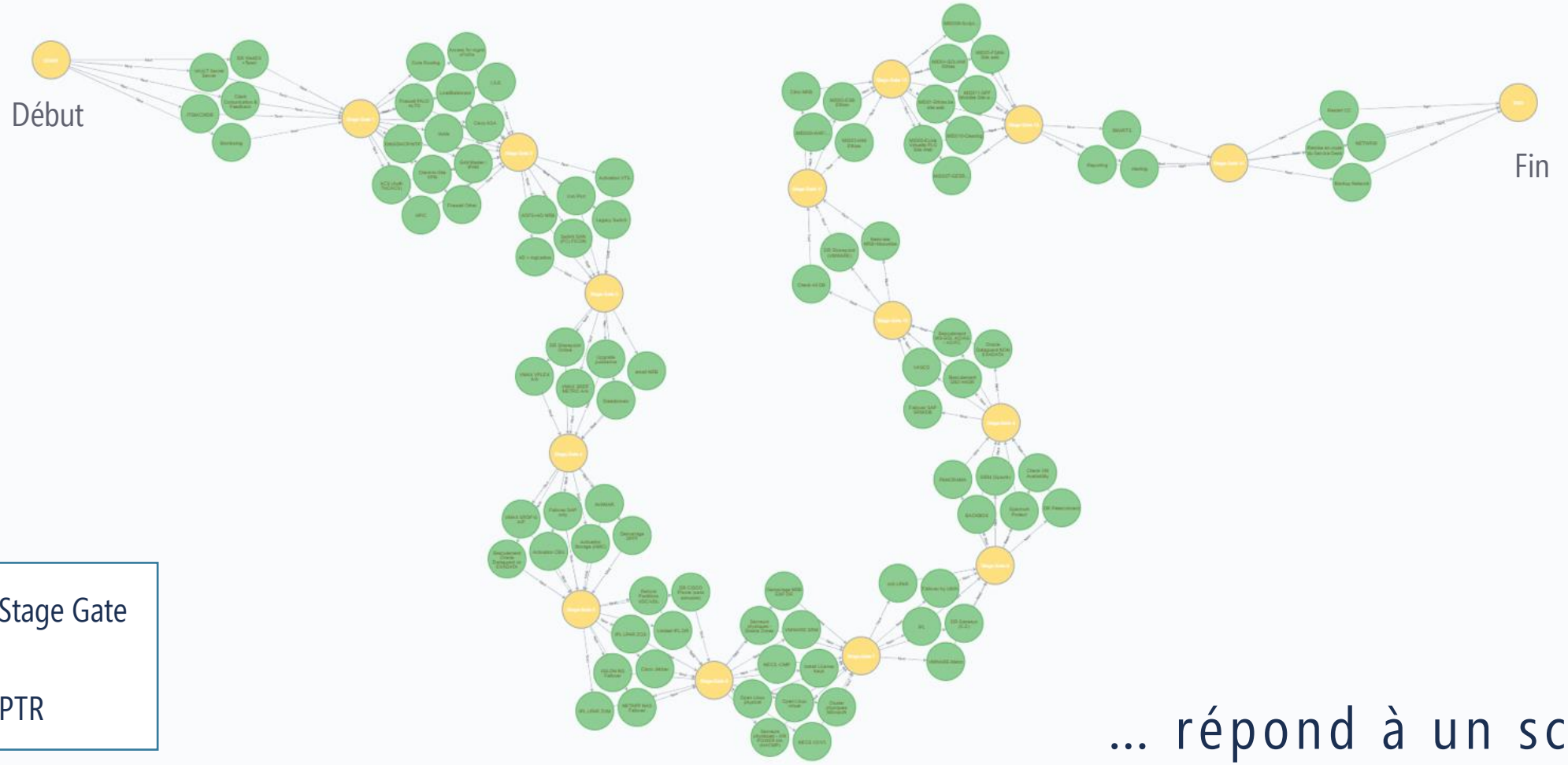


INDICE DE MATURITÉ

MESURER PÉRIODIQUEMENT LA MATURATION DE LA DOCUMENTATION



LE SÉQUENCEMENT DES PTR …



… répond à un scénario

BASCULE TECHNIQUE

Permet de valider la capacité à **basculer** les infrastructures, peu importe la cause, en s'appuyant sur les PTR

VS

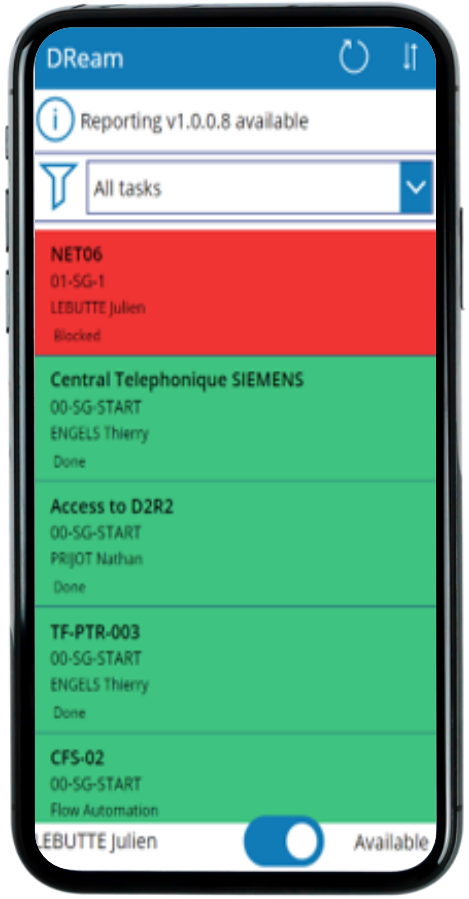
TEST DR

Permet de valider la capacité à **restaurer** des services IT lors d'un scénario s'approchant au mieux d'un sinistre, en s'appuyant sur les PTR

WHAT'S NEXT

DREAM

DISASTER RECOVERY ACHIEVEMENT MONITORING

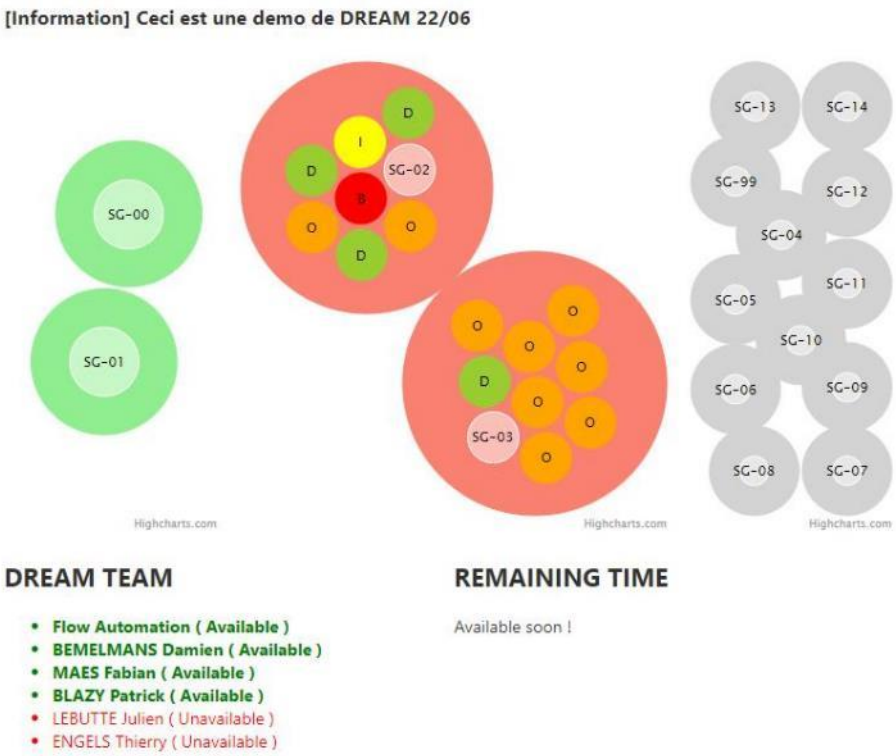


UN OUTIL DE MONITORING :

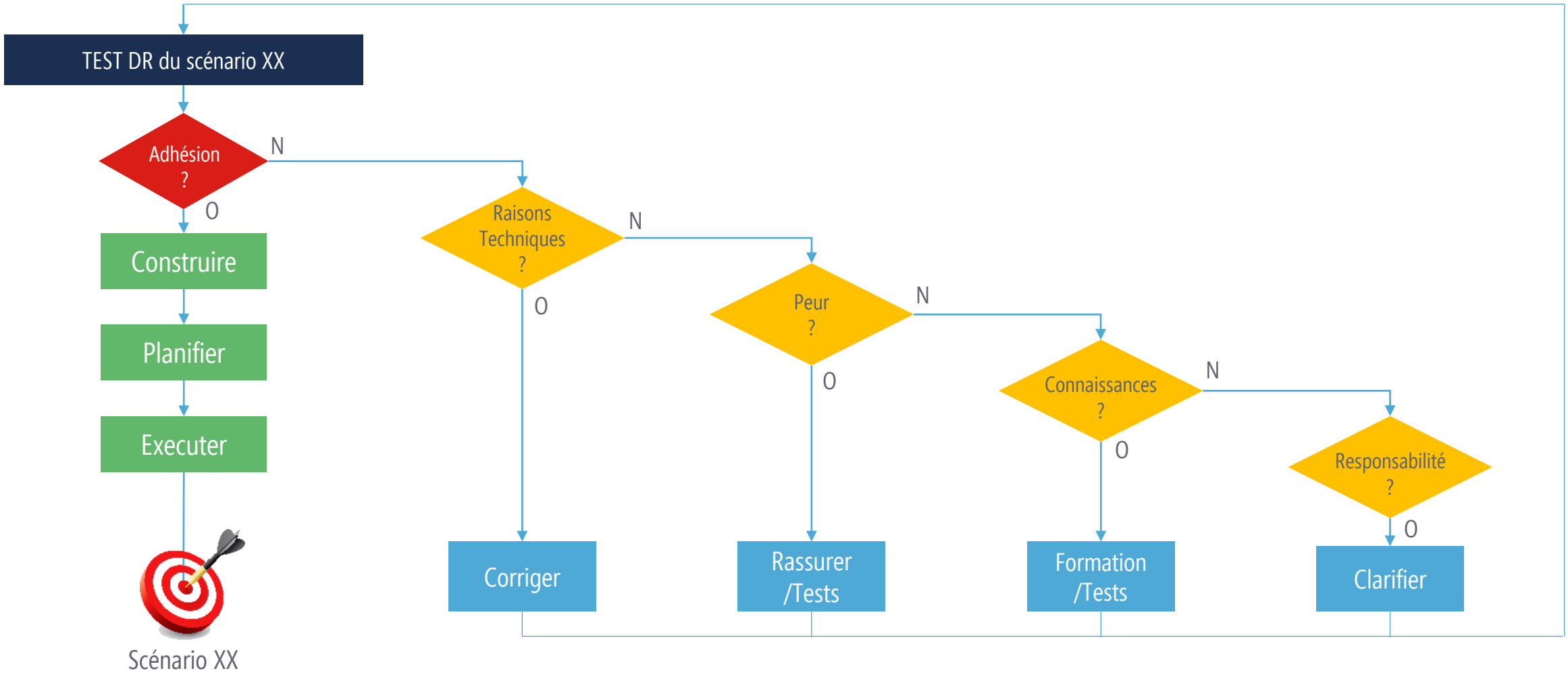
- Suivi du déroulement du plan
- Disponibilité des opérateurs

UNE APPLICATION MOBILE :

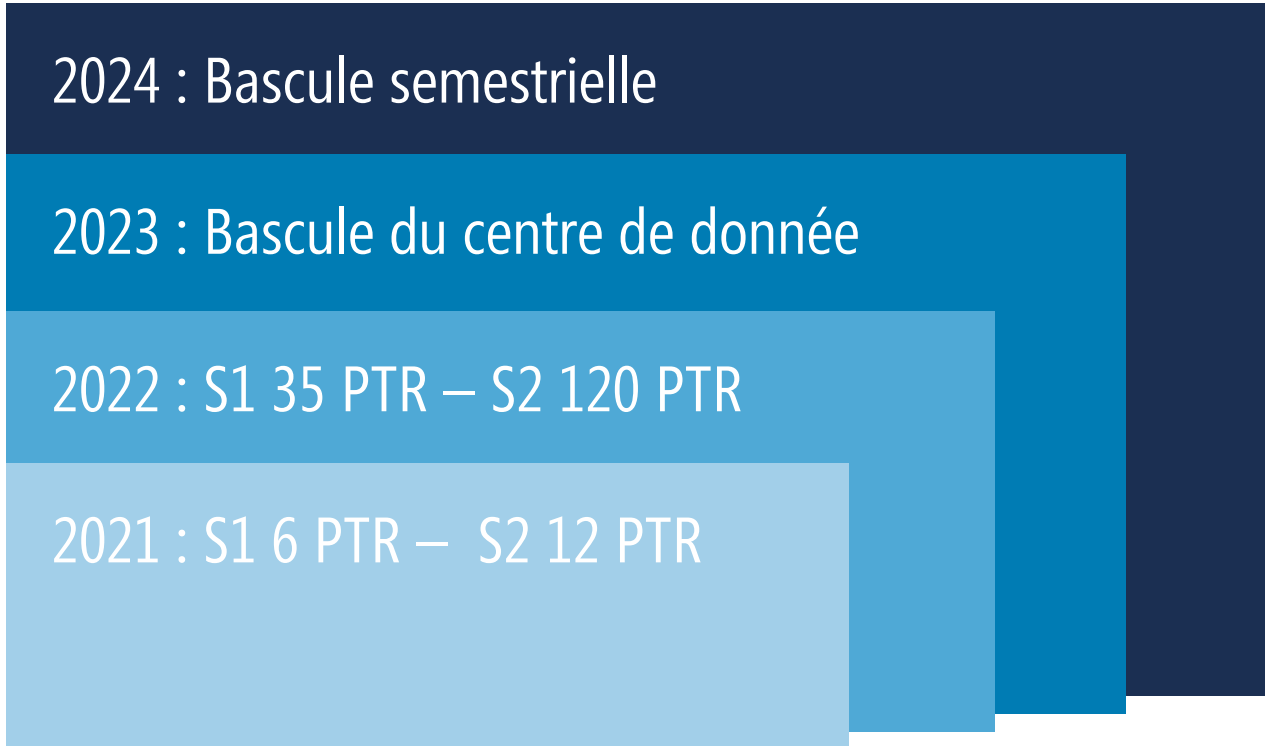
- Suivre l'avancement des opérateurs
- Identifier les blocages
- Calculer les durées de réalisation
- Anticiper les actions
- Prévenir les opérateurs suivants



GARDER LA MOTIVATION, AUGMENTER L'ENTRAINEMENT

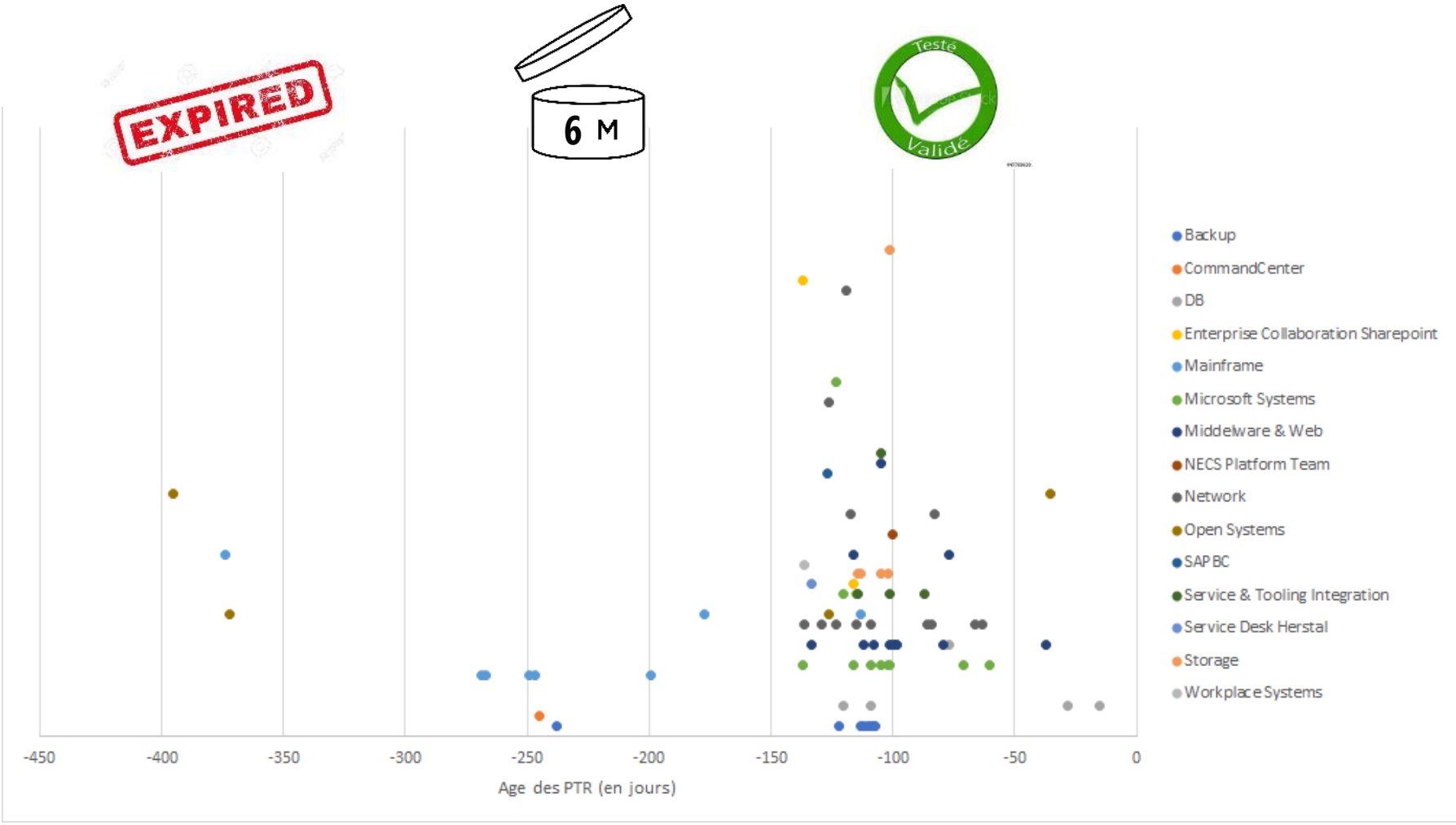


AGRANDIR LE PÉRIMÈTRE

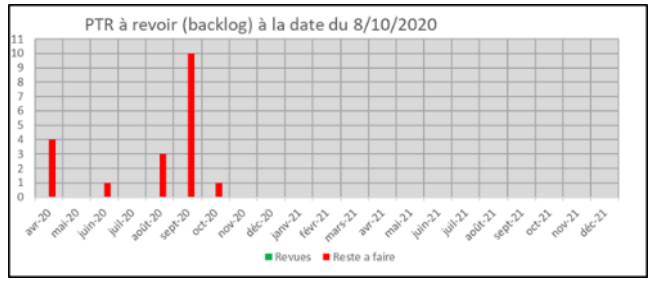


- 2020 : DataCenter
- 2021 : Malware
- 20xx :
  - Pandémie
  - Coupure @
  - Incendie voisinage
  - Perte de données
  - Blocage social
  - Power Outage
  - Coupure GF

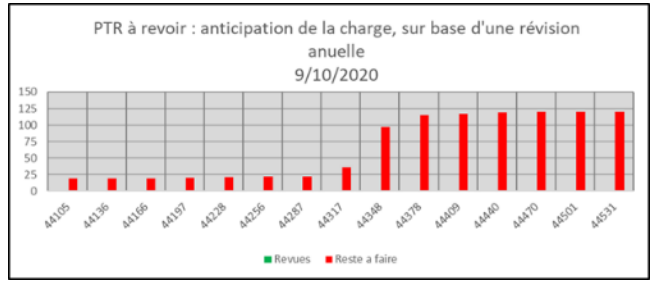
OBSOLESCENCE PROGRAMMÉE



Suivi des backlogs



Anticipation des charges



NRB
DARING TO COMMIT

WHAT'S NEW?

- Une méthodologie
- Bascule Techniques vs Test DR
- Répartition des rôles
- Indices de maturité

WHAT'S NEXT?

- DREAM
- Agrandir le périmètre
- Motivation et entrainement
- Obsolescence programmée


WHAT'S NEW
WHAT'S NEXT
@NRB
Disaster Recovery
Q & R

WHAT'S NEW
WHAT'S NEXT
@NRB

LA QUINZAINE DE NRB DU 23/11 AU 3/12/2020

Marketing@nrb.be
www.nrb.be