ZYROC

Cyber attaques : retour d'expérience sur la remédiation

Mohammed BAKKALI
Didier PILON

1 Octobre 2018

ZYROC

21	21 ans d'expérience chez Microsoft en tant qu'architecte, Premier Mission Critical…
4	4 ans d'expérience à l'ANSSI en tant que Responsables des Opérations de Cybersécurité (ROC)
33	33 opérations de Cyber défense gérées suites à des APT chez des clients grands comptes
+100	Plus de 100 projets de sécurité ou d'identité gérés

Confidentialité

Les différentes phases

5 phases :

1. Initialisation
2. Investigation
3. Préparation
4. Rétablissement sécurisé des services
5. Stabilisation

Phase 1: Initialisation

1 Initialisation

Prise de contact et de contexte

- Présentation du SI
- Nature de la compromission
- Niveau d'impact
- Périmètre(s) identifié(s)
- Contraintes (judiciaires, métiers, …)
- Communication
- Liste des contacts
- Projets en cours et à venir

Analyses du contexte

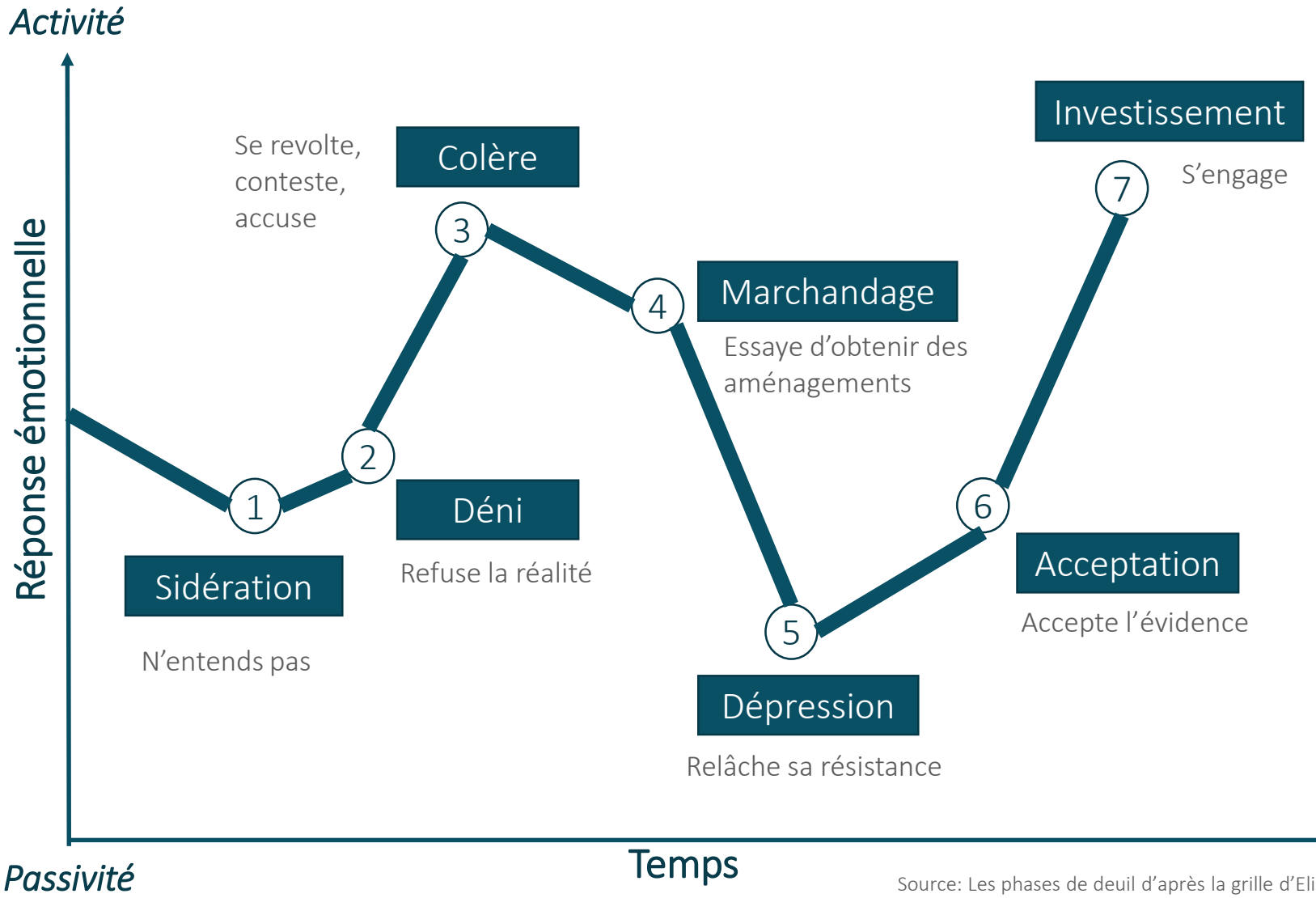
- Identifier et évaluer les risques
- Estimer le niveau de maturité de la victime
- Evaluer le niveau d'acceptation
- Estimer le niveau de connaissance du SI

Décisions

- Définir les objectifs et les conditions de sortie
- Fournir les mesures d'urgence
- Planifier la phase 2

Phase 1: Initialisation

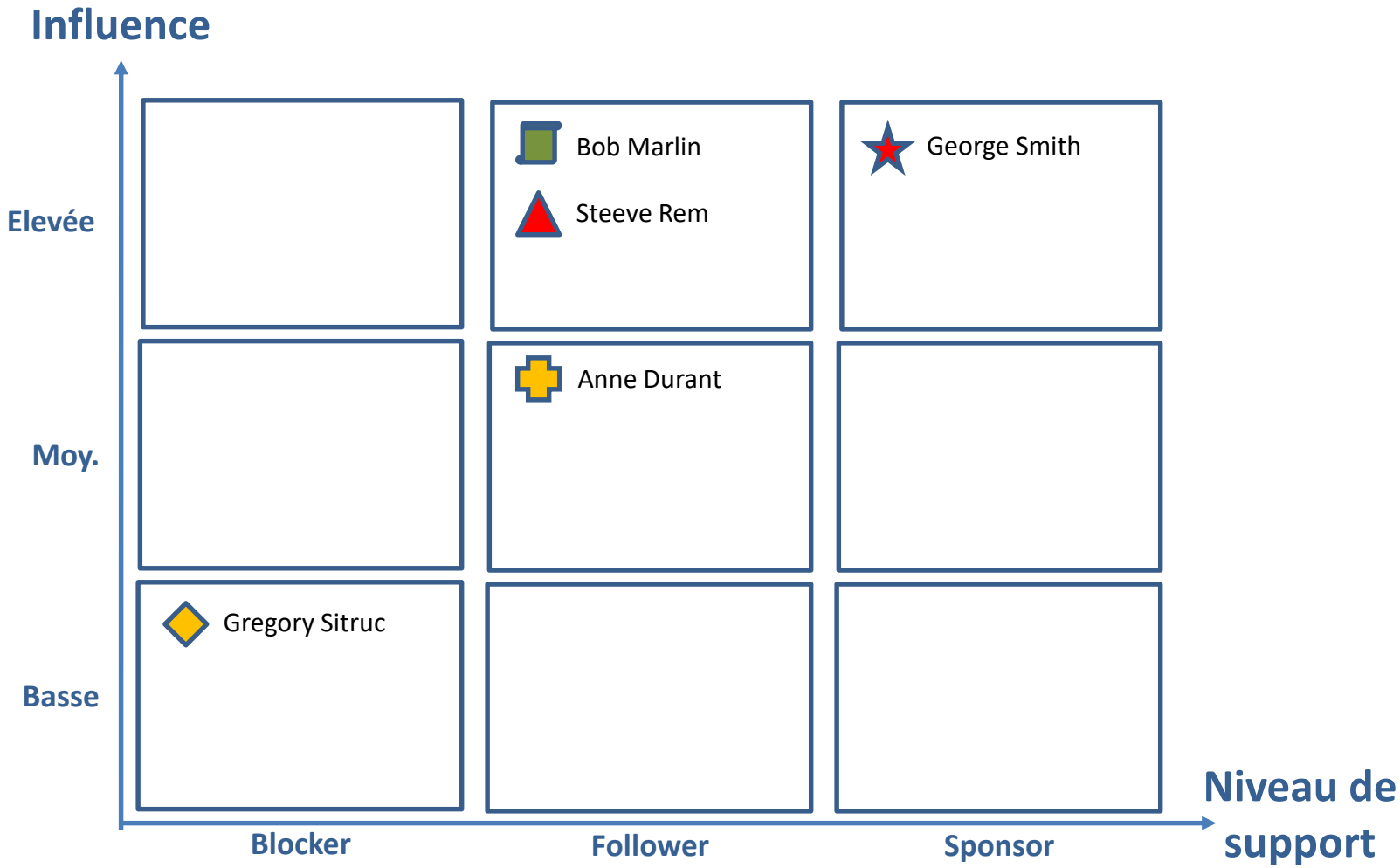
Evaluation du niveau d'acceptation



Source: Les phases de deuil d'après la grille d'Elisabeth Kluber-ROSS

Phase 1: Initialisation

Stakeholder map



Rôles :

- Top management
- Middle management
- Direction de projet
- Sachant technique
- Prestataire

Coopération attendue :

- Nécessaire
- Désirée
- Non indispensable

Phase 1: Initialisation

Exemple d'information de contexte à récupérer

Les acteurs	• Les principaux acteurs coté victime, les prestataires et les fournisseurs de services, les victimes collatérales, …
Juridique	• Judiciarisation, contraintes légales • Le(s) engagement(s) contractuel(s) • …
Métier	• Les contraintes métiers • Les applications et/ou services critiques pour l'entreprise • …
Technique	• L'architecture réseau et système (interconnexion avec d'autres SI, …) • Nombre, type, OS des machines • La liste des applications • Le modèle d'administration • …
Communication	• Plan de communication de crise • Organigramme • …

Phase1: Initialisation

Exemple de mesures d'urgence

- Impliquer le TOP MANAGEMENT
- Vérifier les obligations légales (déclaration d'incident, …)
- Caractériser la compromission (périmètre et MOA)
- Mettre sous sequestre les preuves de la compromission (journaux, dumps mémoire, traces réseau, …)
- Préparer et organiser la communication interne et externe
- Créer une équipe dediée à la résolution de l'incident
- Mettre en place les mesures d'urgence techniques

Phase 2: Investigation

1 Initialisation

2 Investigation

- Réévaluer les objectifs et les conditions de sortie
- Fournir la posture technique
- Planifier la phase 3

Collectes d'informations

- Cartographie (informations techniques)
- Processus et documentations

Analyses

- Analyse du MOA
- Vérification du respect des bonnes pratiques de sécurité
- Forensic des machines compromises
- …

Phase 2: Investigation

Exemple de collecte d'informations

- Informations techniques

Architecture physiques / logiques

Les systèmes d'exploitation

Les services

Les applications

Les 'assets' / données

Le réseau

Le stockage / sauvegarde / archivage

Version
Configuration
Niveau de correctifs
Dépendances
…

Classification, droits, chiffrage, …

- Informations organisationnelles/opérationnelles

Les documents des architectures

Les procédures d'administration/exploitation

Les plans de tests des applications critiques

Les processus

Les acteurs et les partenaires

Les projets en cours et planifiés

Phase 3: Préparation

1. Initialisation
2. Investigation
3. Préparation

Gouvernance de l'affaire
- Organisation des équipes
- Types et fréquences des réunions
- Découpage en plusieurs chantiers
- Planning
- ...

Choix du scénario de remédiation

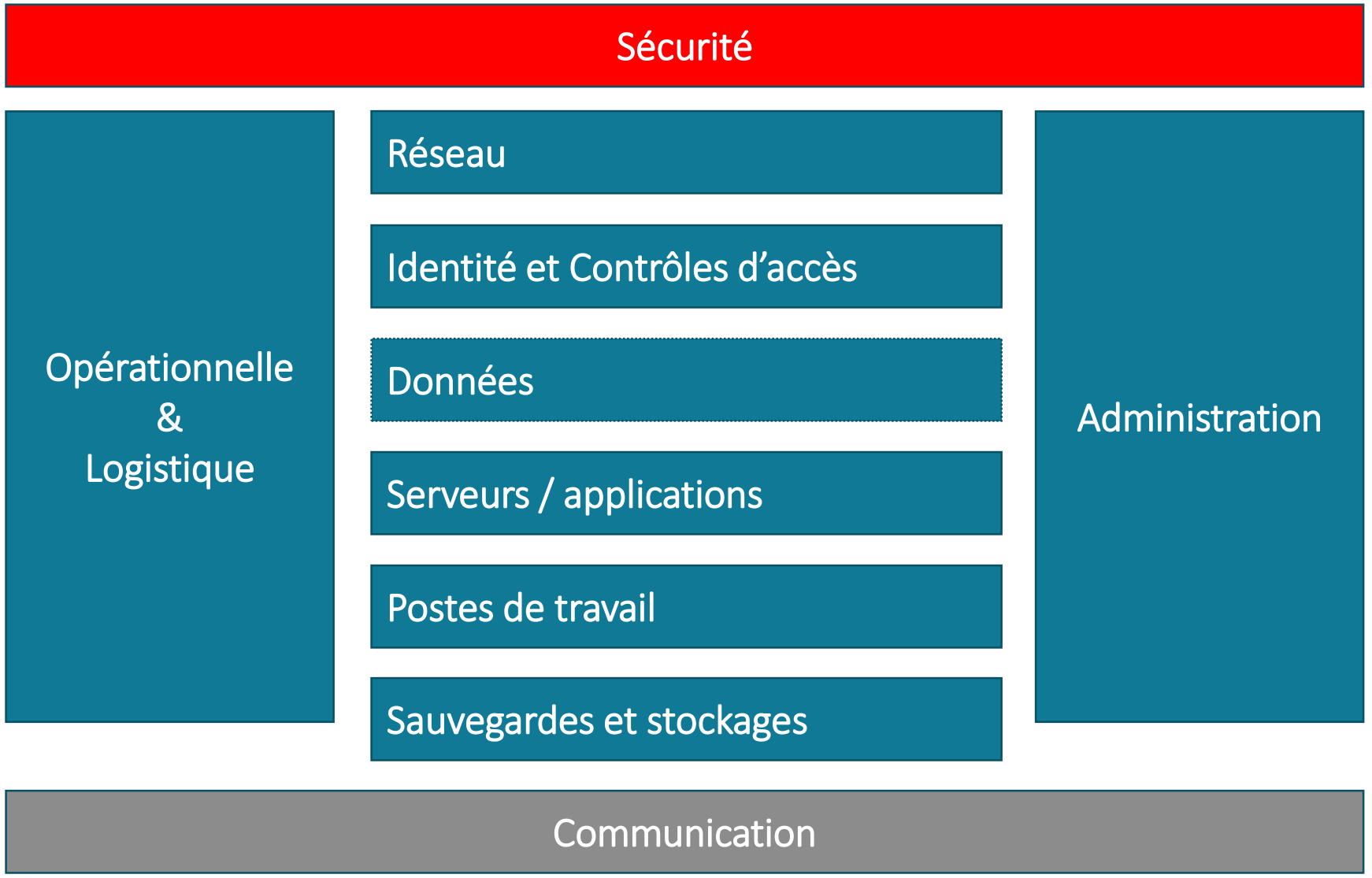
Définition des paramètres de durcissement du SI

Administration des composants sensibles du SI

Communication

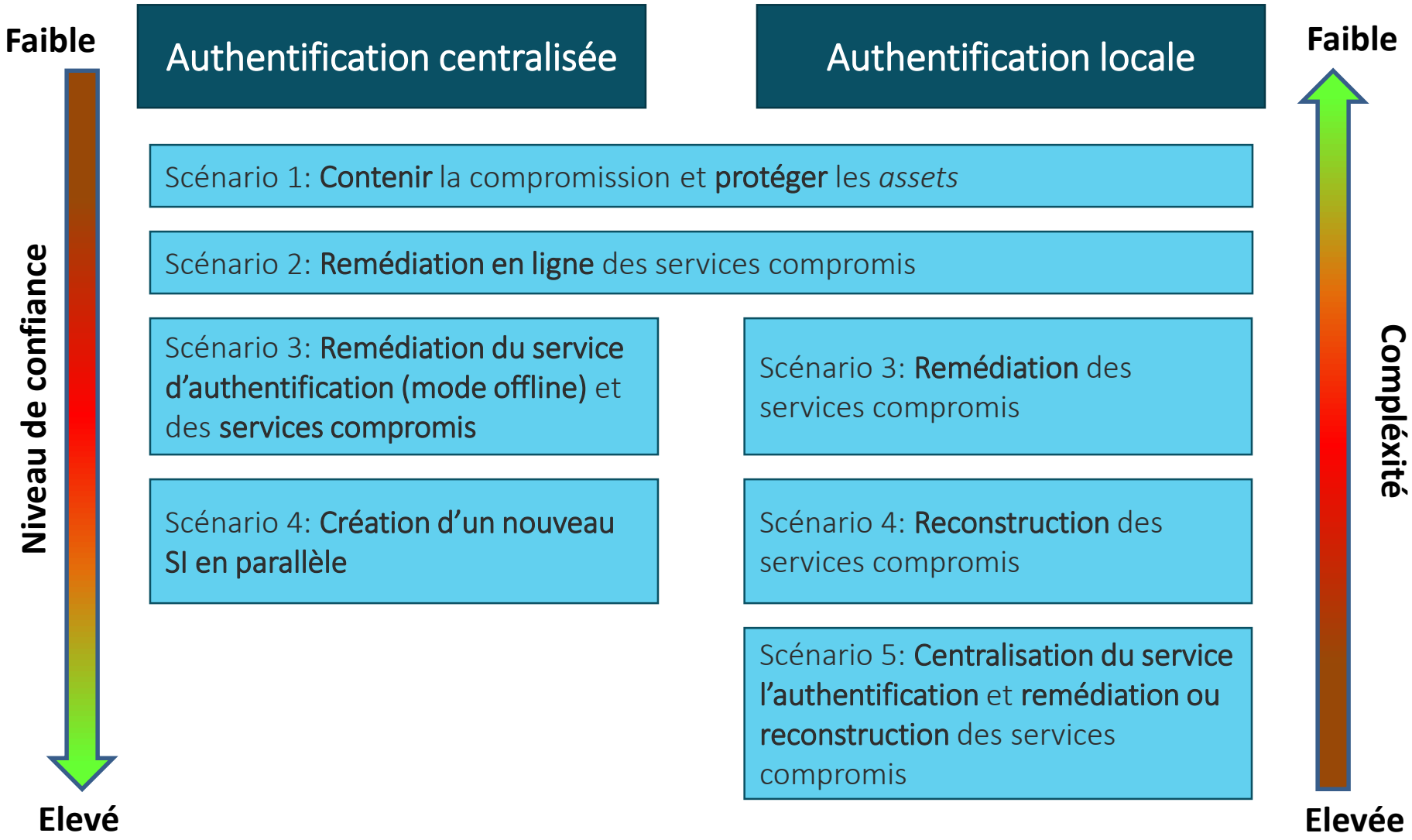
Phase 3: Préparation

Principaux chantiers à traiter



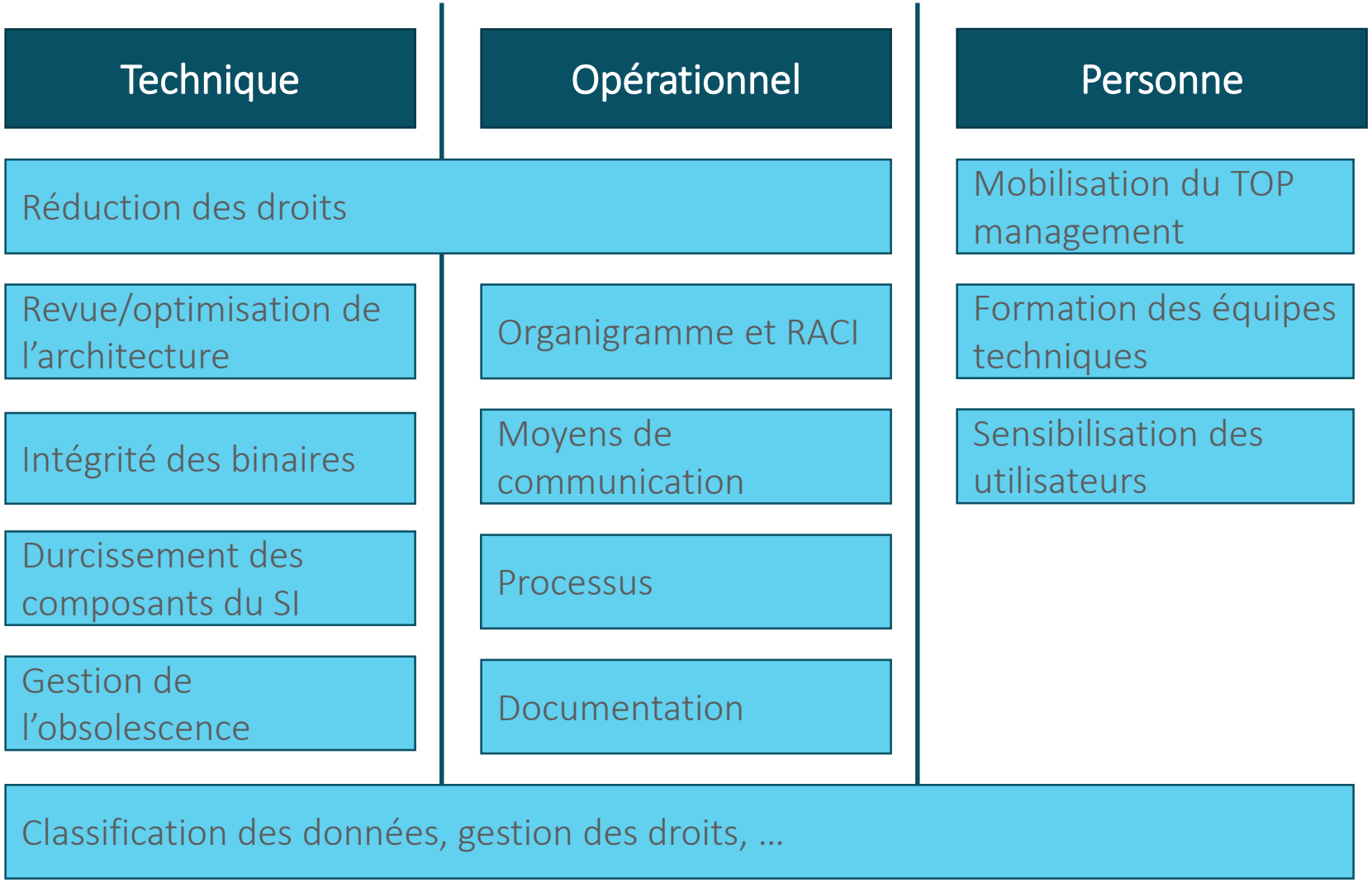
Phase 3: Préparation

Scénarios de remédiation (focus sur la brique Identité et contrôles d'accès)



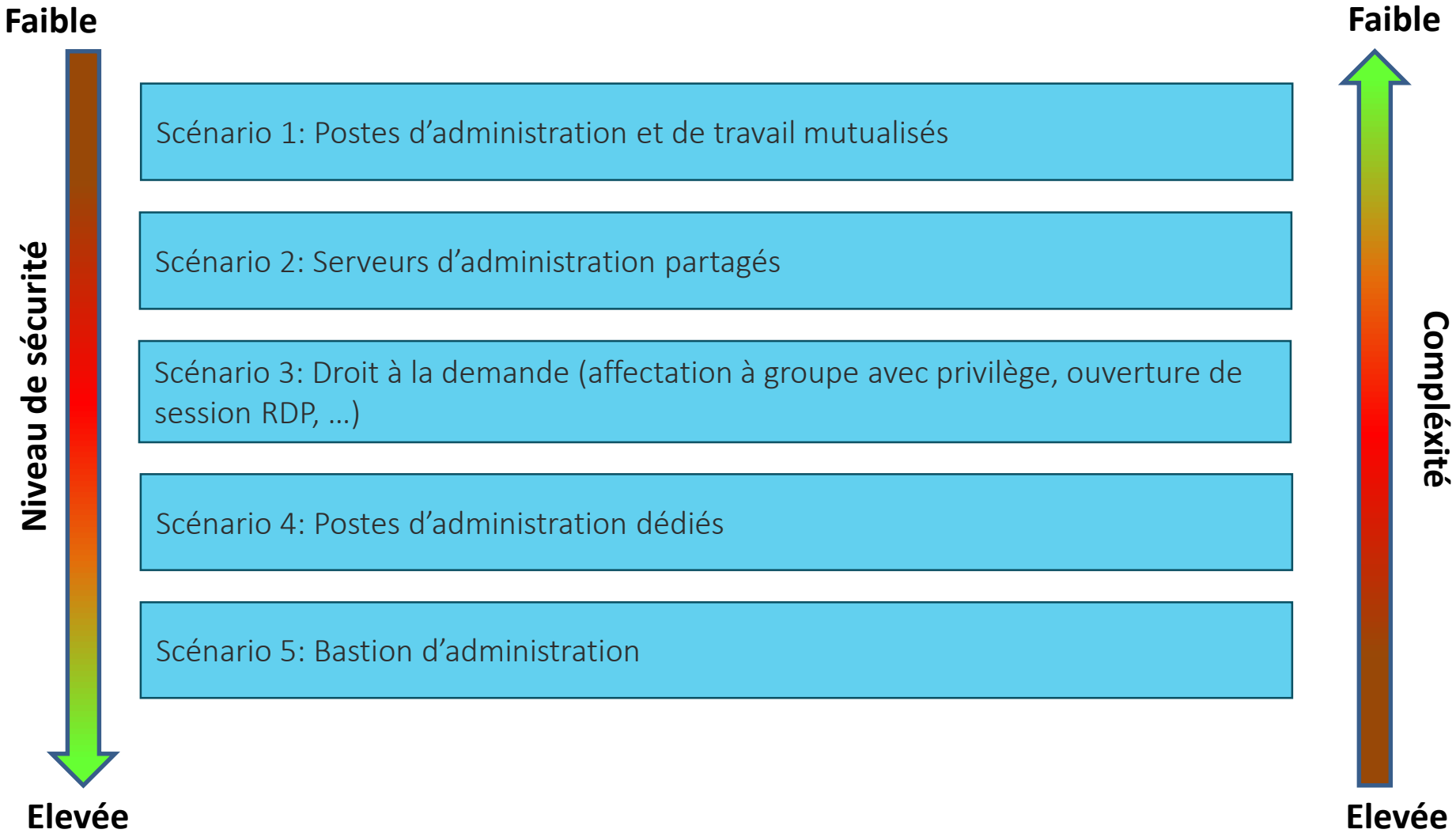
Phase 3: Préparation

Durcir les composants du SI

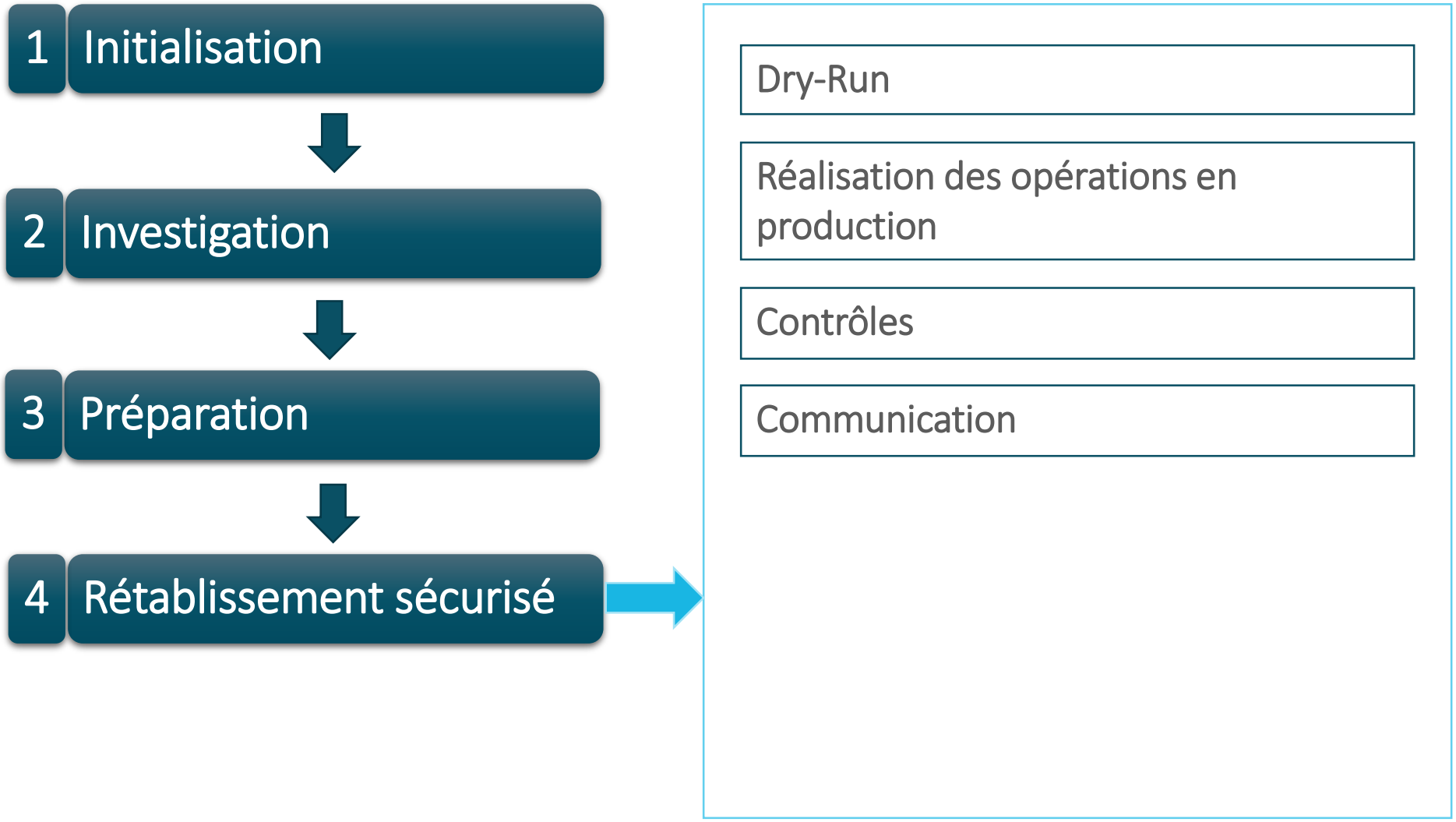


Phase 3: Préparation

Sécuriser l'administration des composants sensibles du SI



Phase 4: Rétablissement sécurisé des services



Phase 5: Stabilisation

- Résolution des incidents
- Supervision
- Contrôle de la conformité
- Formation des équipes techniques
- Sensibilisation des utilisateurs
- Créer et maintenir son plan de reprise d'activité suite à une cyber attaque

Résumé

1. Ne pas se retrouver en mode crise
2. Avoir une bonne connaissance de SI ➔ **Cartographie**
3. Construire des outils et des procédures permettant de rétablir le service et la confiance dans son SI ➔ **Security Recovery Plan (SRP)**
4. Sécuriser son administration ➔ **Bastion d'administration**
5. Durcir son SI et élever le niveau de détection ➔ **Durcissement et traçabilité**
6. Former les équipes IT et sensibiliser les utilisateurs

Merci

Questions ?

Contacts

Didier Pilon
GSM +33 7 70 29 38 79
didier.pilon@zyroc.com

Mohammed Bakkali
GSM +33 6 01 34 10 62
mohammed.bakkali@zyroc.com