V.1.0

Réponse à incident

Séquence 2 : Organisation et gouvernance de crise

OIDANEOS

Processus de gestion de crise

Vision globale

Site primaire

Préparation  Alerte → Diagnostic

Point de ralliement

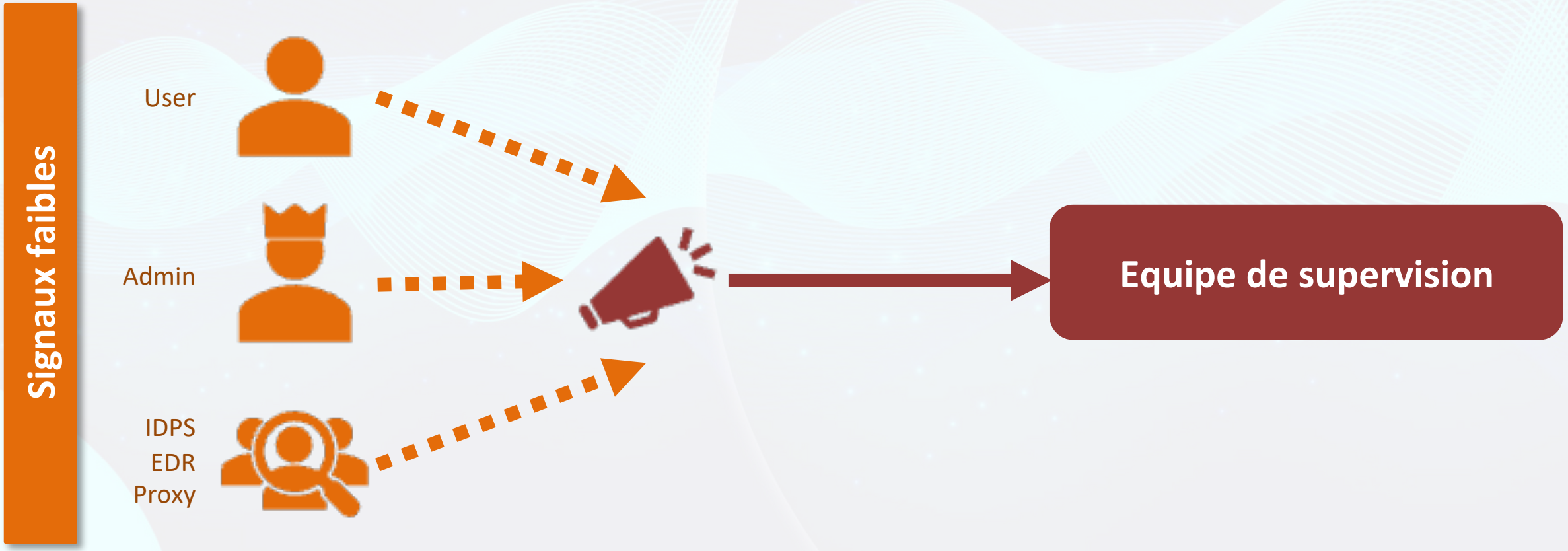
Convocation → Décision

Site de secours

Activation → Reprise → Montée en charge

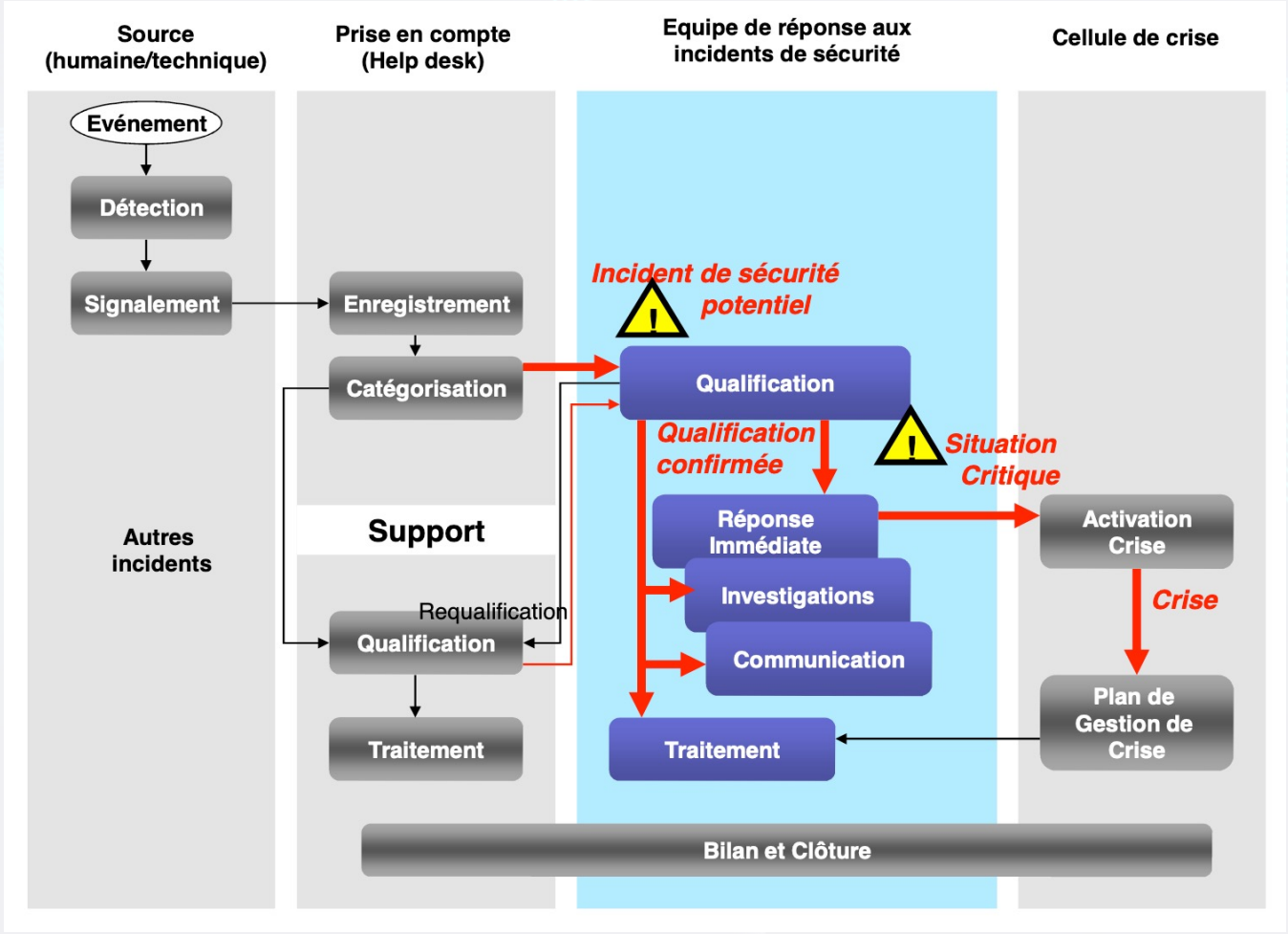
Processus de gestion de crise

Alerte



Processus de gestion de crise

Alerte



Processus de gestion de crise

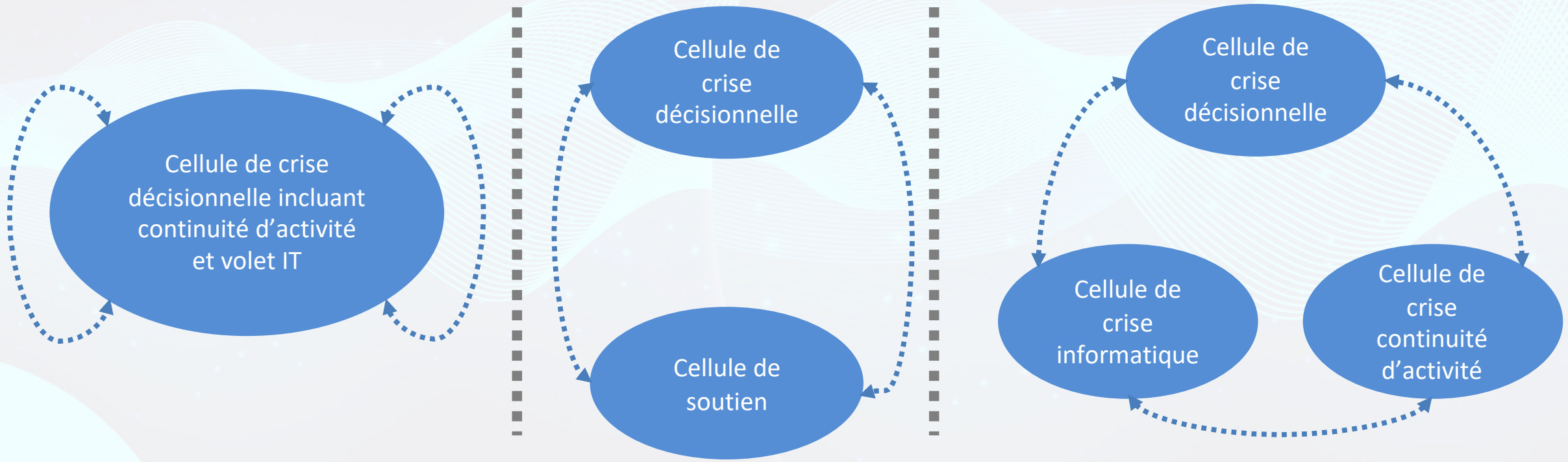
Diagnostic

Type d'incident	Seuil incident mineur	Seuil incident majeur	Seuils de crise
Interruption / indisponibilité du SI x y	x minutes	x heures	y heures
Perturbation du SI x y	x minutes	x heures	y heures
Indisponibilité de Commander ou Livrer	X clients	y clients	z clients
Approvisionnement	Taux de rupture produits x	Taux de rupture produits y	Taux de rupture produits z
Atteinte à la confidentialité des données clients	X clients	y clients	z clients

Exemple de matrice d'évaluation des incidents

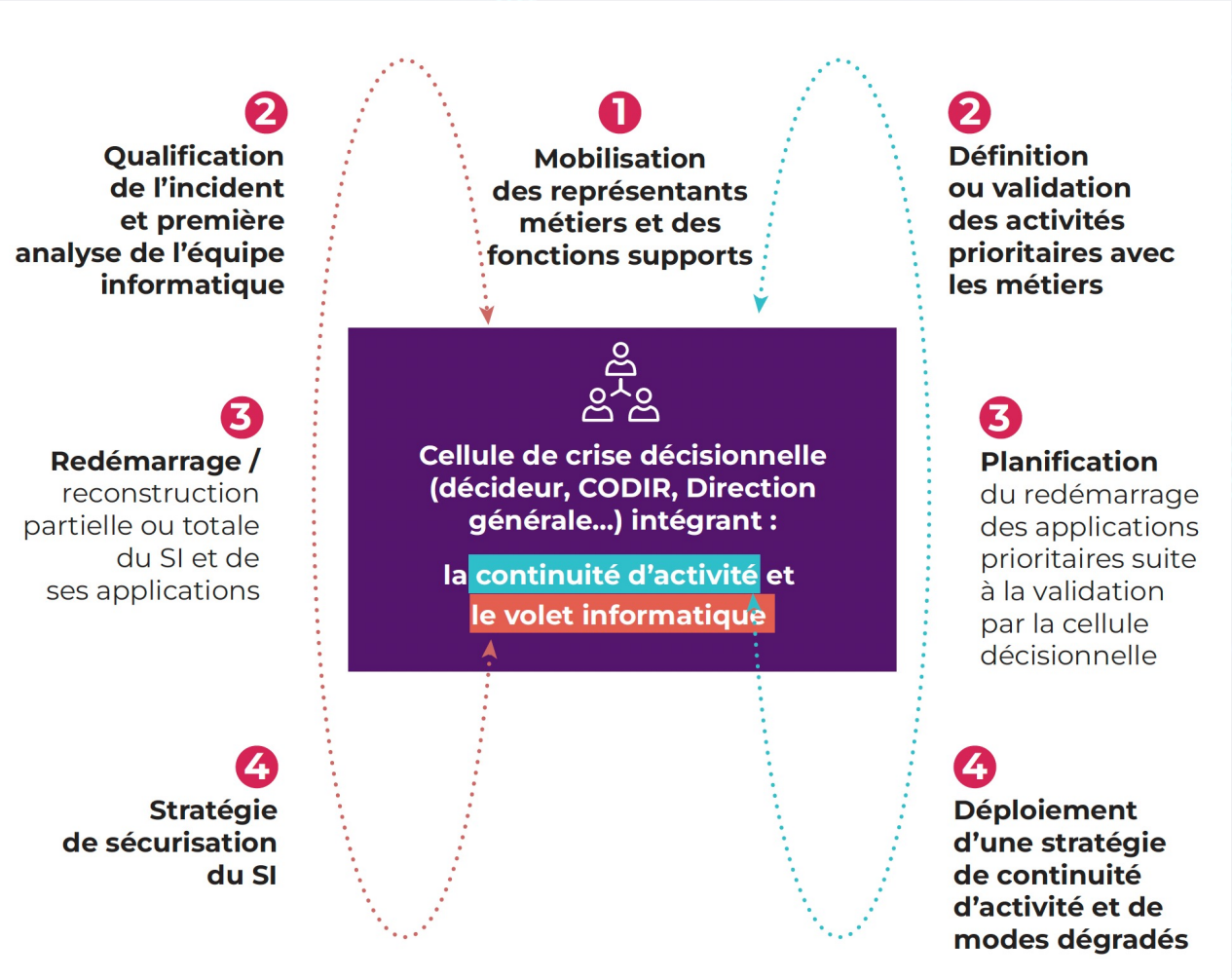
Processus de gestion de crise

Convocation



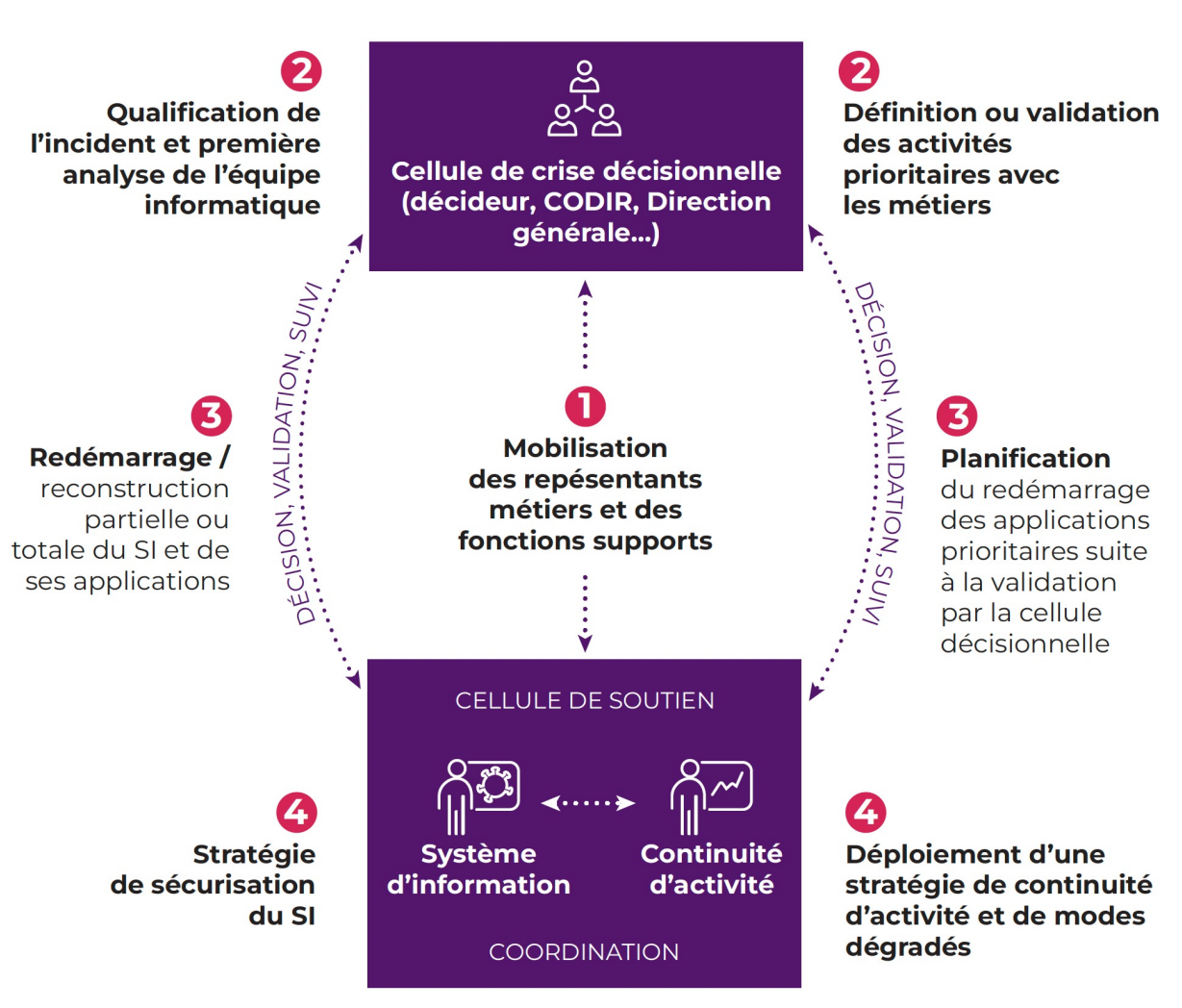
Processus de gestion de crise

Convocation : cellule de crise avec un niveau de maturité faible



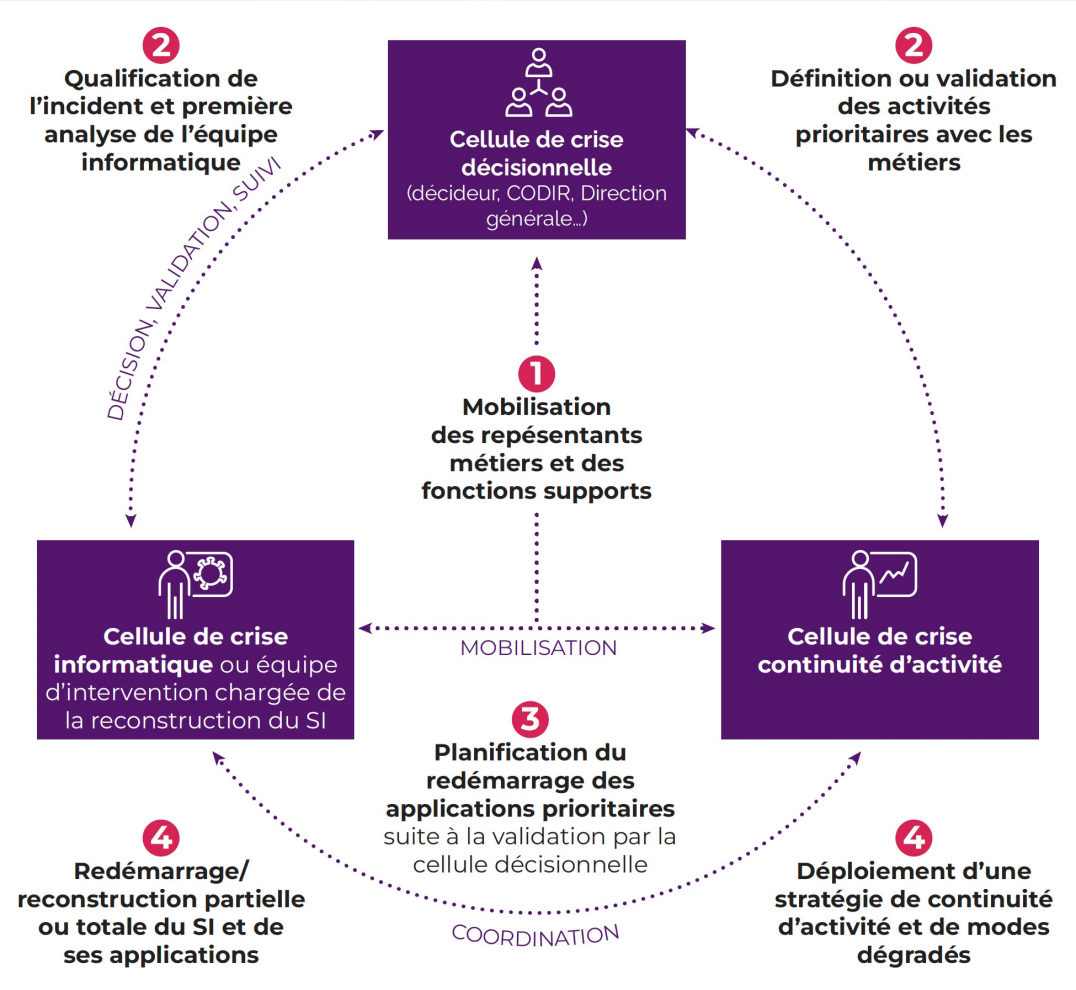
Processus de gestion de crise

Convocation : cellule de crise avec un niveau de maturité intermédiaire



Processus de gestion de crise

Convocation : cellule de crise avec un niveau de maturité élevé



Processus de gestion de crise

Prise de décision

Stratégie de gestion de crise

1. Reconstruction du SI
2. Continuité d'activité métiers

Humain et collectif

Communication de crise

Juridique et règlementaire

Assurance

Gestion multidimensionnelle

Processus de gestion de crise

Prise de décision

Les difficultés pour la prise de décision lors d'une crise

Difficultés	Solutions
Lucidité, rationalité et aptitude du décideur	• Avoir des objectifs précis pour établir un processus de prise de décision adéquat
Visibilité réduite et incertitude	• Avoir une cellule de crise avec les expertises adéquates (SI, continuité métier, anticipation, gestion de crise)

Processus de gestion de crise

Prise de décision : gestion de l'humain et du collectif

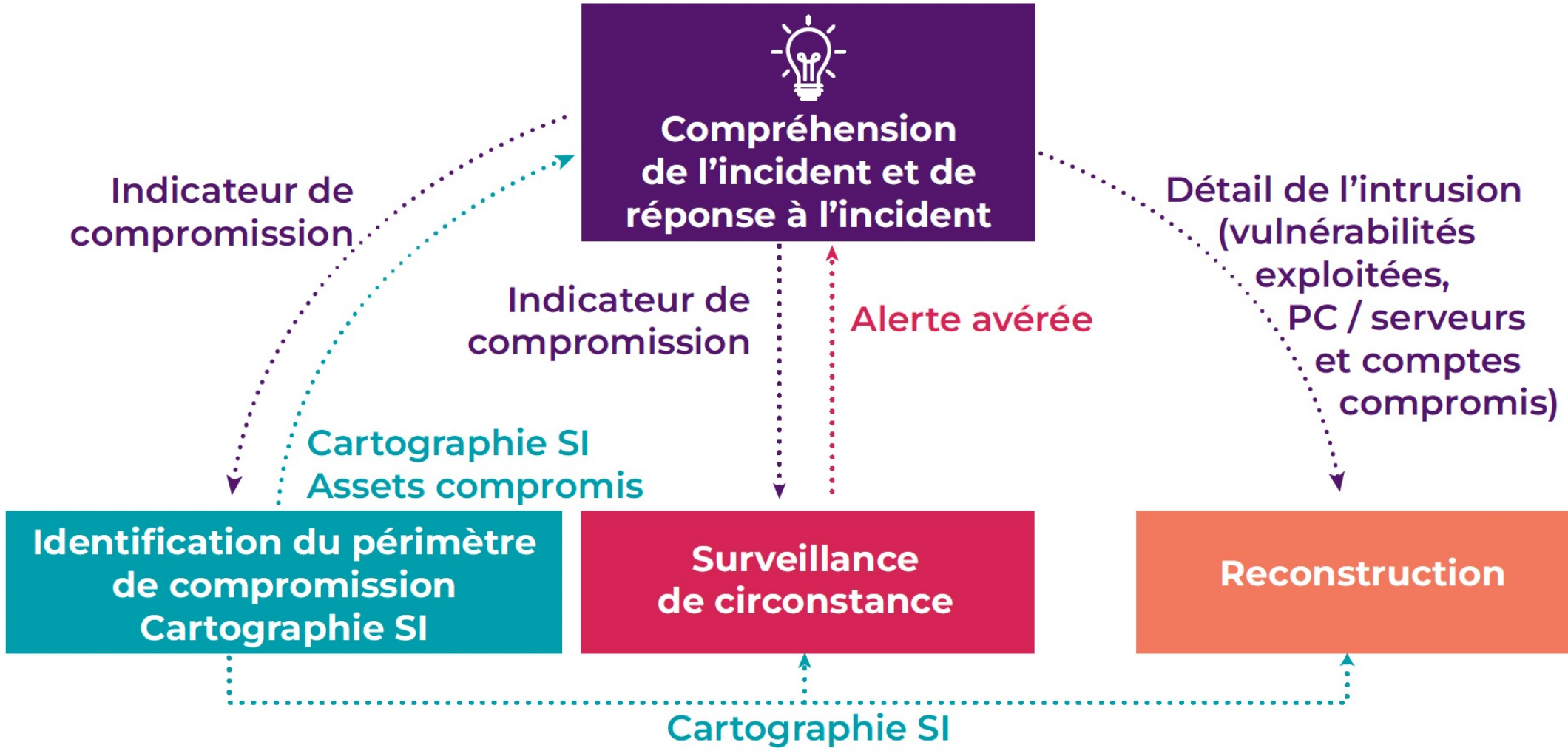
Gestion du stress

Coordination, mise en réseau et échange d'information

Dynamique collective

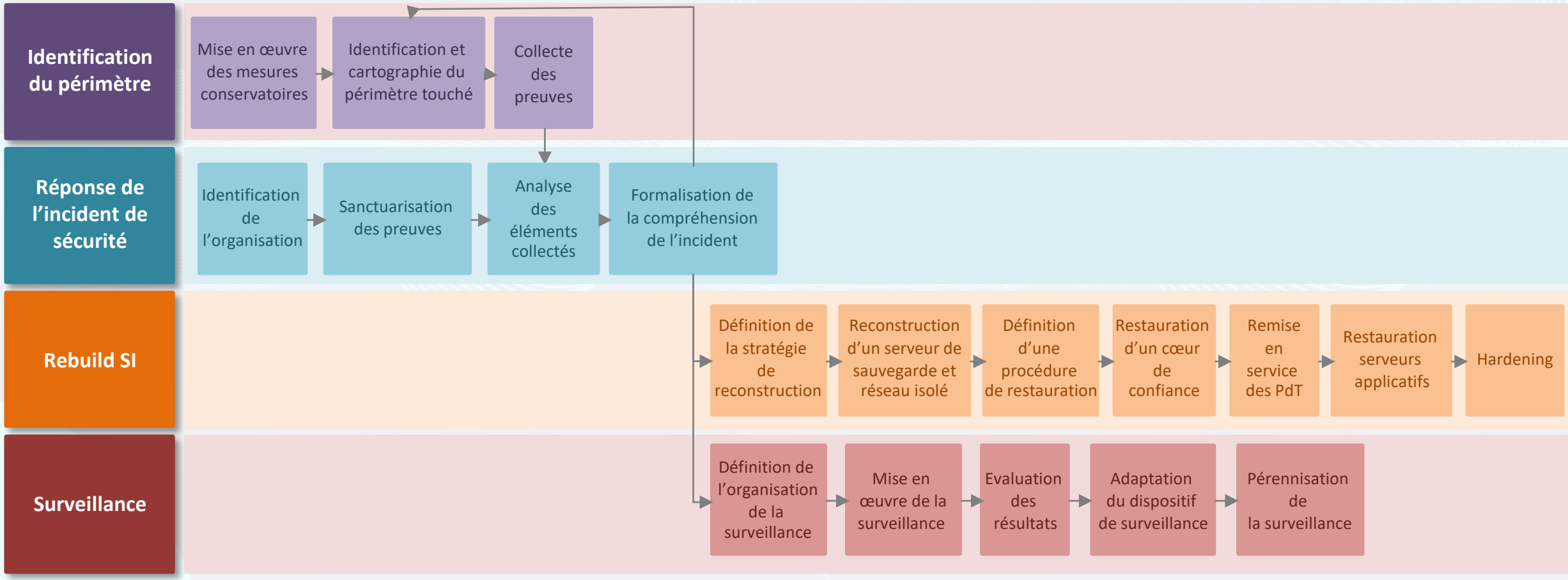
Processus de gestion de crise

Reprise



Processus de gestion de crise

Reprise



Processus de gestion de crise

Reprise : stratégie de compréhension et de réponse à incident

Organisationnel

Identification des contacts pertinents :

- Responsable de la cellule de crise DSI
- RSSI
- Responsable de production ou des infrastructures
- DPO

Technique

Eléments et preuves pour aider à la compréhension initiale :

- Cartographie du SI
- Schéma d'architecture
- Journaux d'événements, antivirus, réseaux (archivés et centralisés)
- Domaine AD existants

Processus de gestion de crise

Reprise : sanctuarisation des preuves

Ne pas éteindre les machines pour ne pas perdre les informations contenues dans les processus en mémoire

Une machine chiffrée peut contenir des éléments de preuve utiles

Préférer une approche conservatoire qu'un redémarrage des serveurs

Processus de gestion de crise

Reprise : sanctuarisation des preuves

Collecte d'informations

- Liste des fichiers présents
- Processus en cours d'exécution
- Journaux à disposition
- Contenu de la RAM
- Traces réseau
- Supports de stockage

Identification des éléments

- Dates (au format UTC)
- Outils / techniques et artefacts pour identifier l'agent de menace
- Adresse IP et noms de domaines
- Comptes compromis
- Autres machines compromises

Augmentation du périmètre de crise

- Nouvelles machines compromises
- Dates antérieures aux dates actuellement connues
- Marqueurs dans les journaux globaux disponibles

Rédaction d'un rapport d'analyse

- Timeline
- Actions menées par l'agent de menace
- Potentielles vulnérabilités exploitées
- Indicateurs de compromission
- Machines compromises
- Comptes compromis

Processus de gestion de crise

Reprise : sanctuarisation des preuves

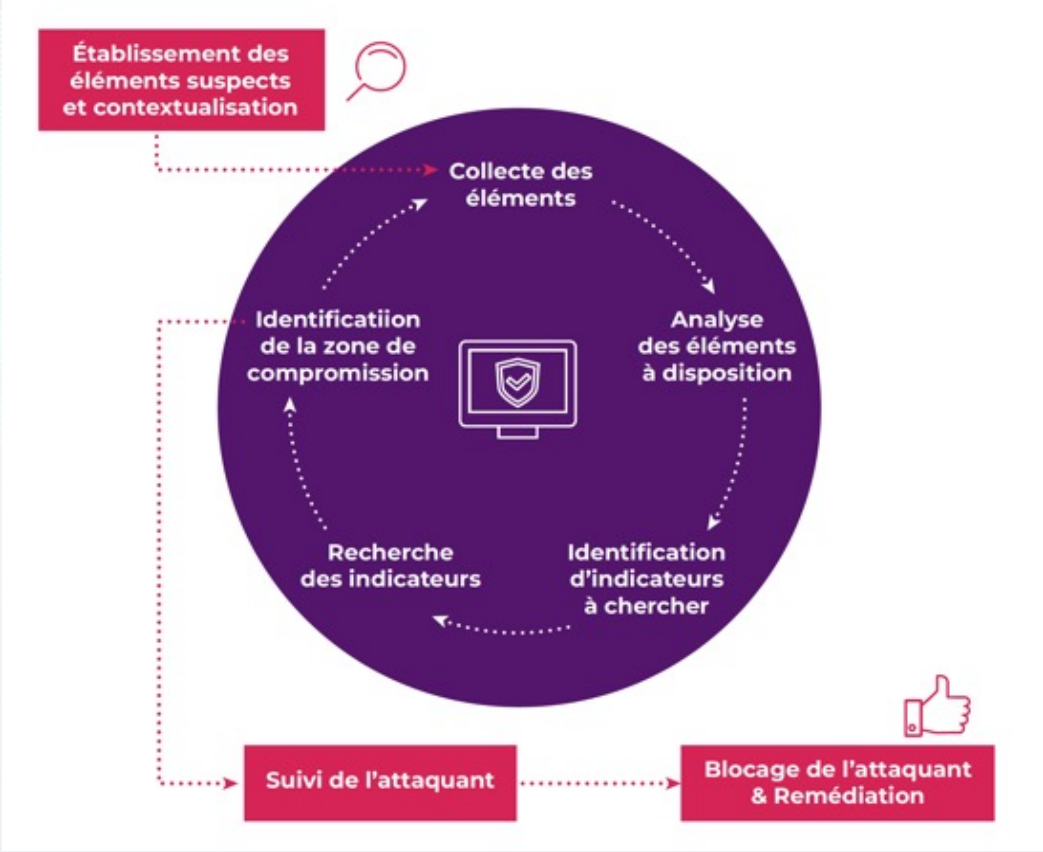
Eléments récoltés	Aide à la reconstruction saine
Timeline et date de compromission initiale	Déterminer l'ancienneté des sauvegardes qu'il faudra restaurer
Indicateurs de compromission	Assurer l'intégrité des machines et serveurs recréés
Vulnérabilités exploitées	Connaître les actions de sécurisation du SI à mener

Processus de gestion de crise

Reprise : identification du périmètre de compromission

Décrire les éléments qui peuvent faciliter le travail de l'équipe d'investigation

- Sanctuarisation des journaux réseaux et des contrôleurs de domaines AD
- Caractérisation de la nature de l'attaque
- Evaluer l'état des systèmes de stockage et sauvegarde
- Identifier le périmètre compromis observable et les systèmes ayant pu être attaqués par rebond
- Evaluer les impacts opérationnels et domaines fonctionnels altérés du SI
- Collecter les indicateurs de compromission
- Rassembler la documentation



Processus de gestion de crise

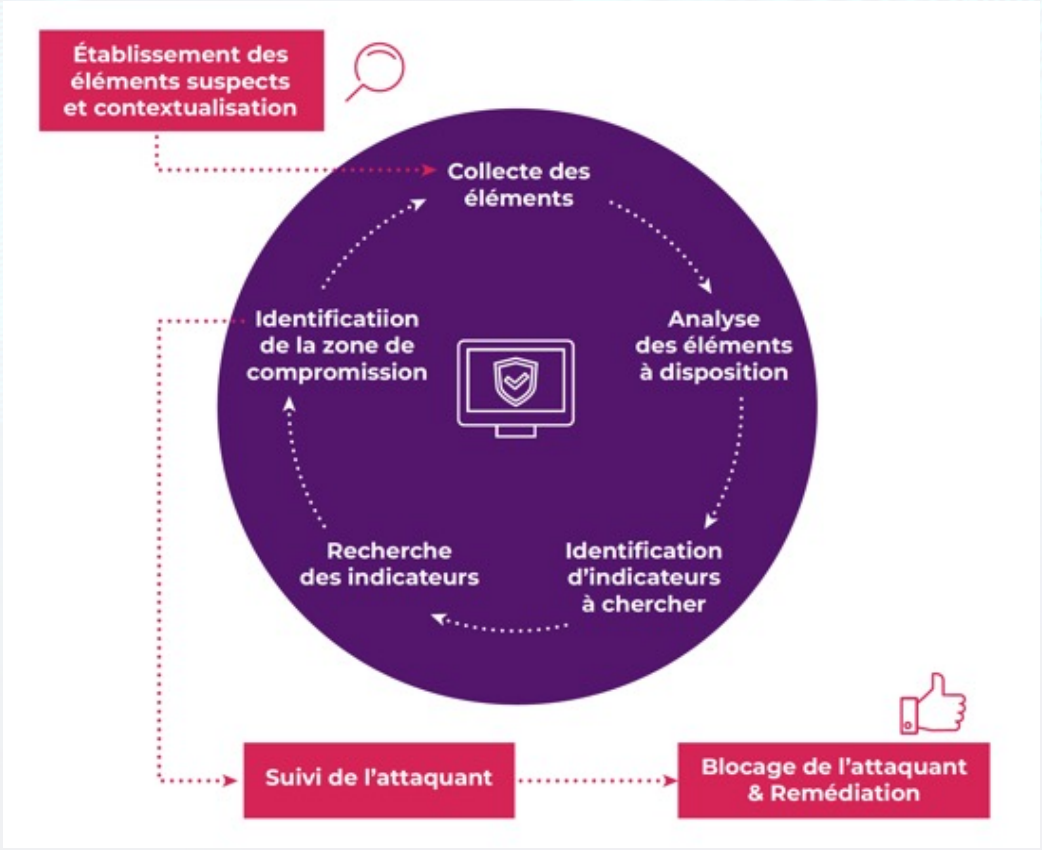
Reprise : identification du périmètre de compromission

Application des mesures conservatoires

- Mise à l'abri des journaux systèmes et réseaux
- Isolation des réseaux vis-à-vis des réseaux tiers non compromis et vis-à-vis d'Internet
- Isolation des serveurs
- Interdiction de la mise sous tension des terminaux éteints au moment de l'attaque

Collectes d'informations complémentaires

- Acquisition de mémoire de processus, de médias de stockage
- Acquisition d'artefacts (journaux, exécutables, traces réseaux…)



Processus de gestion de crise

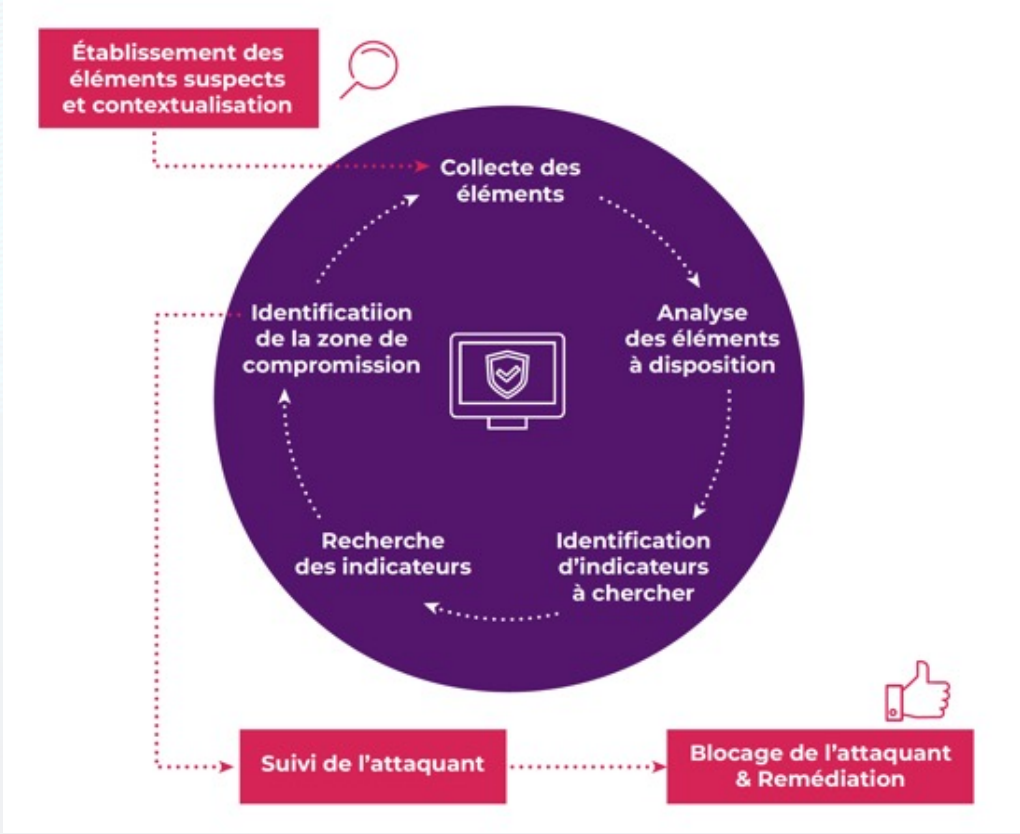
Reprise : identification du périmètre de compromission

Recherche des indicateurs

Sur les journaux à disposition ou le SI en cours de fonctionnement

Sur le réseau compromis mais aussi sur le réseau reconstruit

Partageable pour recherche avec des partenaires



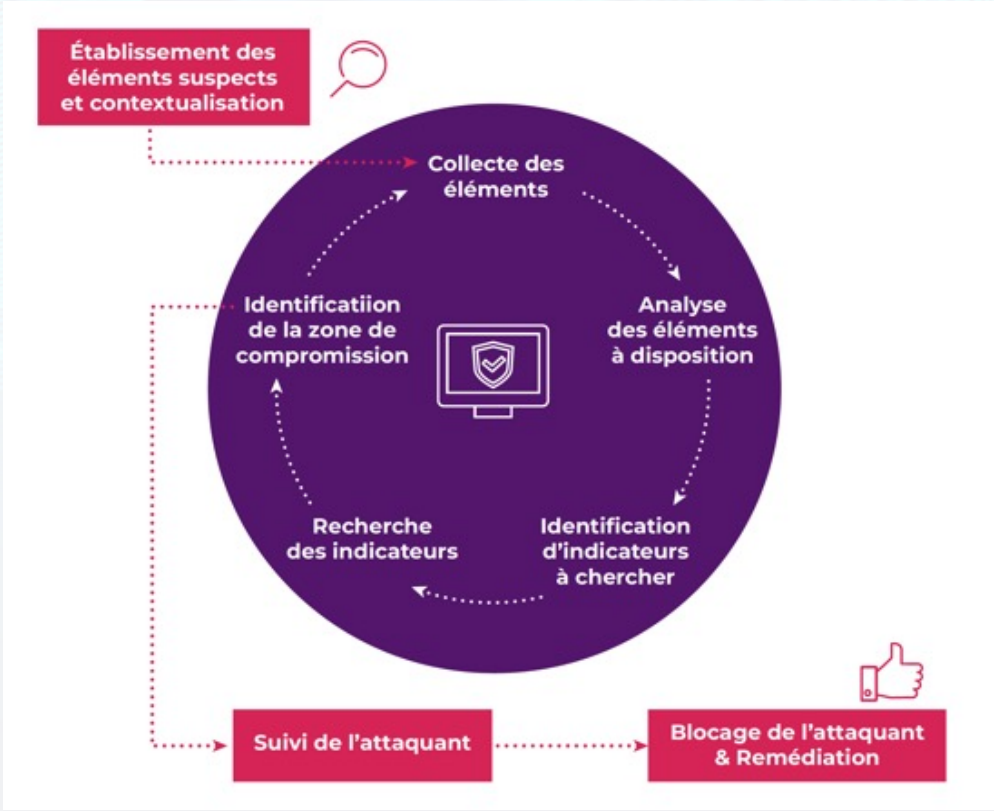
Processus de gestion de crise

Reprise : identification du périmètre de compromission

Identification de la zone de compromission

De potentiels nouveaux systèmes compromis peuvent être identifiés

Dans le cas de la découverte de nouveaux systèmes compromis, il faut refaire une collecte d'éléments



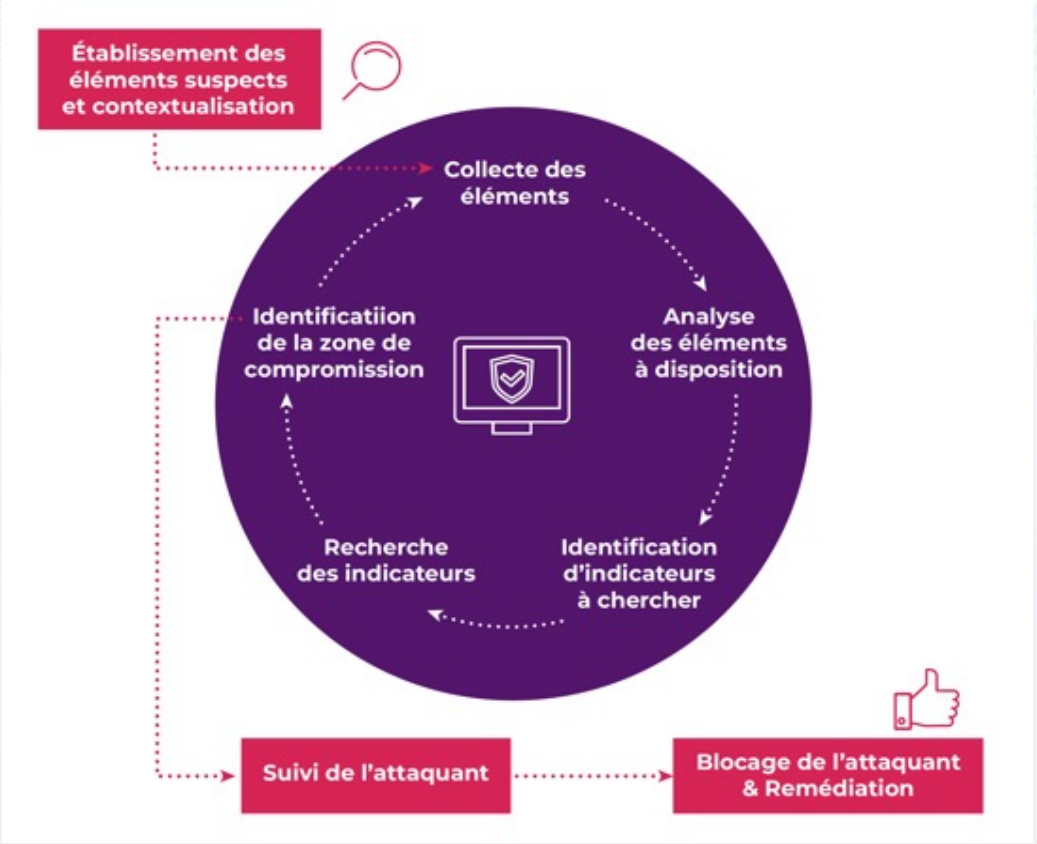
Processus de gestion de crise

Reprise : identification du périmètre de compromission

Suivi de l'agent de menace

Superviser les actions de l'attaquant (s'il est encore actif)

Réalisation de cette activité dans certains cas à évaluer avec les capacités de la victime et des experts forensiques



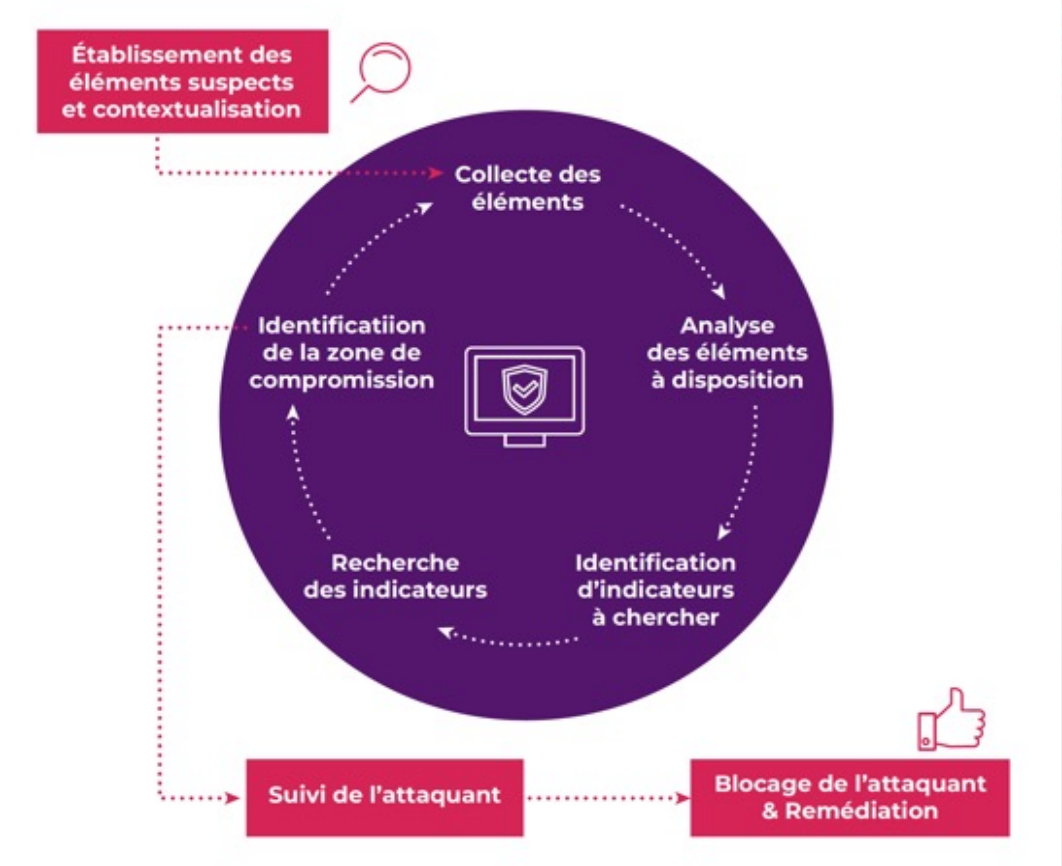
Processus de gestion de crise

Reprise : identification du périmètre de compromission

Blocage de l'agent de menace et remédiation

Déconnexion totale des communications avec l'extérieur du SI

Remédiation simultanée ou bascule vers un système sain



Processus de gestion de crise

Reprise : stratégie de reconstruction du SI

Prérequis nécessaires pour la reconstruction

Avoir une vision claire de l'état des sauvegardes ou des mécanismes de restauration

Identifier la date de la dernière sauvegarde des systèmes et données

Repérer les outils déposés par l'attaquant et les comptes qu'il a compromis ou créés

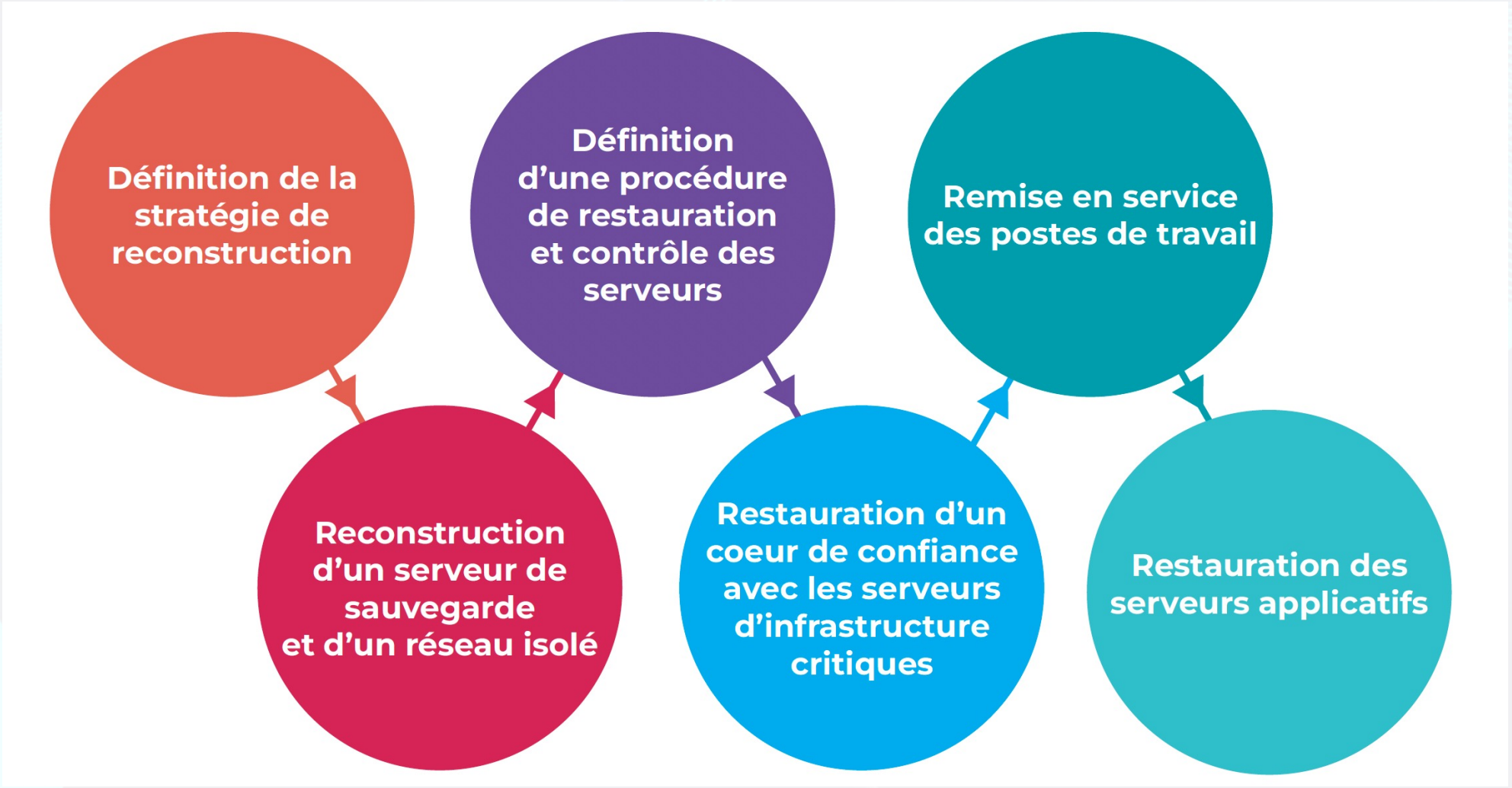
Comprendre les vulnérabilités exploitées durant l'attaque

Disposer de nouveaux postes de travail ou postes d'administration

Isoler le réseau d'Internet

Processus de gestion de crise

Reprise : stratégie de reconstruction du SI



Processus de gestion de crise

Reprise : stratégie de reconstruction du SI – scénarios de reconstruction

Sauvegardes avant la date de la compromission et d'intrusion

- Pas de code malveillants
- Risque de perte de données
- Actions de sécurisation nécessaires

Dernière sauvegarde du SI

- Systèmes restaurés potentiellement compromis
- Procédure de nettoyage et de vérification nécessaire

Reconstruire le SI de zéro

- Repartir sur des bases saines et sécurisées
- Temps de reconstruction important
- Risque de perte définitive des données

Processus de gestion de crise

Reprise : stratégie de reconstruction du SI – étapes de reconstruction

Etape 1

Remise en place du serveur de sauvegarde

- Isolation du nouveau serveur de sauvegarde
- Réalisation de tests de sauvegarde
- Désactivation du système de purge / rotation

Etape 2

Procédure de Sanity Check

- Définir une procédure de contrôle de l'état du serveur

Etape 3

Restauration des serveurs d'infras critiques

- Serveurs DNS/DHCP
- DC AD
- Serveurs d'authentification
- Console d'administration

Etape 4

Remise en service des postes de travail

- Réinstallation ou restauration des postes chiffrés
- Les actions à mener vont dépendre du parc de postes à restaurer

Etape 5

Restauration des serveurs applicatifs

- Convertir les besoins métiers en liste de serveurs
- Identifier les chaines infras associés
- Suivre la procédure de contrôle de l'état santé du serveur
- Faire attention à la cohérence des données et à reconstituer les données perdues

Processus de gestion de crise

Reprise : stratégie de reconstruction du SI – étapes de reconstruction

Hardening du SI

Campagne de patchs critiques sur les composants critiques

Migration des OS obsolètes

Authentification forte pour les accès distants

Postes admins distincts des postes bureautiques

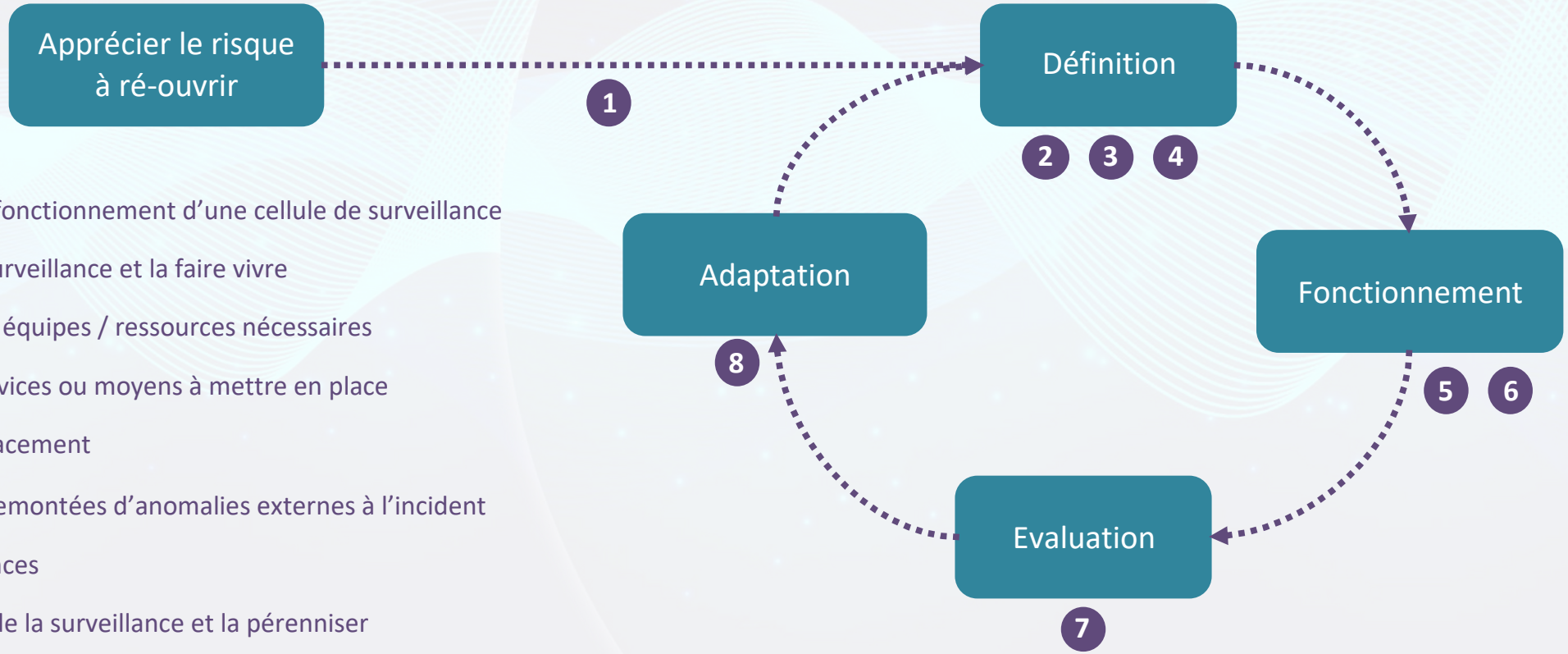
Restriction des flux réseaux entrants

Renforcement de la politique de filtrage Internet

Liste blanche pour les accès Internet sur les serveurs

Processus de gestion de crise

Reprise : surveillance de circonstance



1. Définir les objectifs et le fonctionnement d'une cellule de surveillance
2. Constituer la cellule de surveillance et la faire vivre
3. Identifier et mobiliser les équipes / ressources nécessaires
4. Eléments à surveiller, services ou moyens à mettre en place
5. Comment surveiller efficacement
6. Comment réagir sur les remontées d'anomalies externes à l'incident
7. Indicateurs de performances
8. Tirer les enseignements de la surveillance et la pérenniser

Processus de gestion de crise

Reprise : surveillance de circonstance

1 Définir les objectifs et le fonctionnement d'une cellule de surveillance

Eviter une aggravation de la situation

Vérifier que l'attaque est bien contenue

Capable d'alerter la cellule de crise en temps réel

Processus de gestion de crise

Reprise : surveillance de circonstance

2 Constituer la cellule de surveillance et en assurer le pilotage

Définir
l'organisation

Mettre en place
une gouvernance

Processus de gestion de crise

Reprise : surveillance de circonstance

3 Identifier et mobiliser les équipes / ressources nécessaires à la surveillance

- Identifier les ressources en amont
- Répartir les missions au niveau des relais terrain
- Répartir les missions au niveau des relais terrain

Processus de gestion de crise

Reprise : surveillance de circonstance

4 Eléments à surveiller, services ou moyens à mettre en place

Journaux (FW, proxy, VPN)

Sondes réseaux

Annuaires et systèmes d'administration

Serveurs

Postes d'administration et postes de travail

Serveurs de messagerie

Stockage / sauvegarde

Applications métiers critiques

Processus de gestion de crise

Reprise : surveillance de circonstance

4 Eléments à surveiller, services ou moyens à mettre en place

Utilisation de services supplémentaires externalisables

CERT (interne ou externe)

Prestataire de réponse à incident

Services de détections

Mode de paramétrage des outils de détection

Suivi de correction des vulnérabilités exploitées

Surveillance du darkweb pour identifier les fuites de données

Processus de gestion de crise

Reprise : surveillance de circonstance

5 Comment surveiller efficacement

Equipe de surveillance dédiée

Alimenter les équipes sur les techniques et vulnérabilités exploitées

Mettre à jour le tableau de bord de gestion de crise

Allouer les moyens techniques et RH nécessaires

Processus de gestion de crise

Reprise : surveillance de circonstance

6 Réaction sur des remontées d'anomalies externes à l'incident

Remontée d'événements de sécurité hors attaque

▼

Prioriser les incidents liés à l'attaque et consigner les autres événements de sécurité

Processus de gestion de crise

Reprise : surveillance de circonstance

7 Indicateurs de performance

Taux de couverture du SI

Taux de déploiement des solutions de sécurité

Volume d'alertes générées et traitées

Pourcentage de faux positif

Répartition des alertes (liés ou non à l'attaque)

Processus de gestion de crise

Reprise : surveillance de circonstance

8 Tirer les enseignements de la surveillance

- Organisation à mettre en place
- Compétences requises
- Dimensionnement
- Types d'outils de surveillance
- Liens avec les entités

Processus de gestion de crise

Montée en charge : sortie de crise et bilan

Opportunité pour l'organisme de mieux se structurer et de tirer des enseignements

Communication

- Communication avec les collaborateurs et parties prenantes
- Remerciement des personnes mobilisées
- Proposition d'un accompagnement psychologique

Bilan à chaud

- Partage du ressenti de chacun
- Premier retour pour dégager les premières conclusions

Structuration

- Aide à la réalisation du retour d'expérience

Processus de gestion de crise

Montée en charge : retour d'expérience

- Dossier de suivi
- Synthèse des bonnes et mauvaises pratiques
- Actions correctives
- Plan d'action
- Amélioration des dispositifs de mesure de sécurité
- Mesures préventives
- Revue des procédures actuelles
- Evaluation de l'impact de la crise

Processus de gestion de crise

Montée en charge : retour d'expérience

Organiser un REX dans un délai d'un mois maximum avec les acteurs de la gestion de crise

1. Mener des entretiens
2. Respecter la chronologie
3. S'appuyer sur le journal de crise
4. Recenser les points forts
5. Recenser les difficultés
6. Lister les actions d'amélioration à réaliser
7. Mettre en place des solutions
8. Bâtir le plan d'actions associé

Processus de gestion de crise

Montée en charge : retour d'expérience

Retour d'expérience

- Evénements et alerte
- Entrée en crise
- Logistique
- Cadrage de la situation et évaluation des impacts
- Fonctionnement de la cellule de crise
- Prise de décision

- Relations avec les parties prenantes externes
- Communication interne et externe
- Retour à une activité normale
- Communication post crise
- Etat des lieux de la situation actuelle

Retour d'expérience

Processus de gestion de crise

Montée en charge : capitalisation

Feuille de route d'amélioration de la SSI

- Renforcement des capacités humaines
- Identification des chantiers de sécurité
- Mise en place d'un budget cybersécurité

Processus de gestion de crise

Montée en charge : capitalisation

Cadrage des grandes lignes des projets

Identification des prérequis nécessaires

Estimation budgétaire

Construction d'un plan projet

Processus de gestion de crise

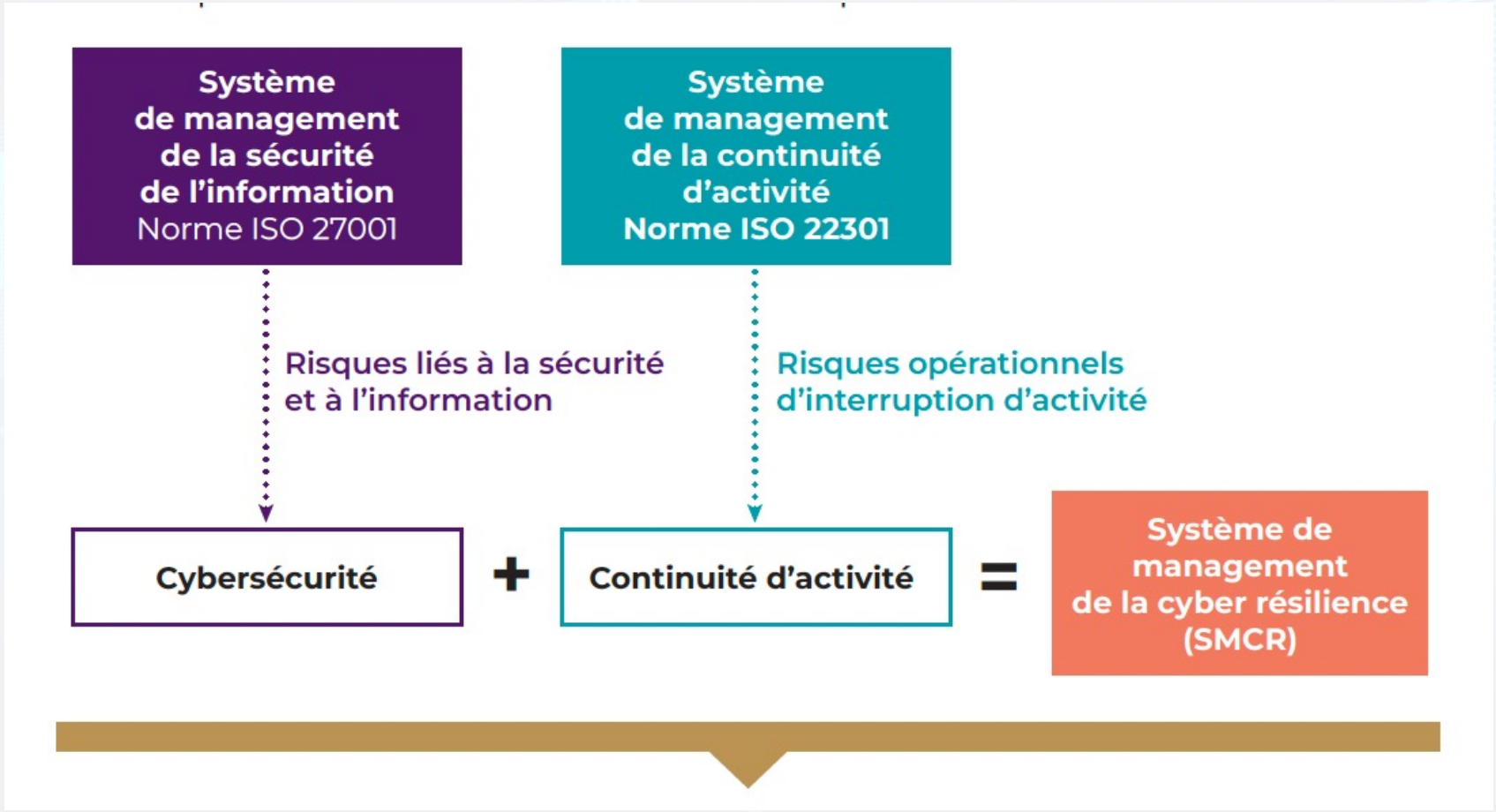
Montée en charge : capitalisation

Evaluer l'efficacité du PCA / PRA ou mettre en place un PCA/PRA

- Elaborer et valider les modes dégradés
- Réaliser ou mettre à jour la cartographie des risques / BIA
- Réalisation de tests, d'exercices et de simulations
- Partager le RETEX avec les autres décideurs

Processus de gestion de crise

Montée en charge : capitalisation



Processus de gestion de crise

Exemple : IRM ADVENS / SG

myCERT | aDvens

IRM (Incident Response Methodologies)

CERT aDvens provides easy to use operational incident best practices in french from the CERT Societe Generale IRMs.

These cheat sheets are dedicated to incident handling and cover multiple fields in which a CERT team can be involved.

One IRM exists for each security incident we're used to dealing with.

These cheats sheets have been written in English with CERT Societe Generale Team, translate into French.

CERT aDvens would like to thank CERT SG who accepted our contribution to update these cheat sheets.

Feel free to contact us if you identify a bug or an error in these IRMs.

This work is licensed under a Creative Commons Attribution 3.0 Unported License.