Aide à la gestion de crise

Cyberattaque

Novembre 2021

INTRINSEC

Innovative by design

TOUR CBX, 20ème ETAGE, 1 PASSERELLE DES REFLETS, 92913 PARIS LA DEFENSE CEDEX • TEL +33 1 41 91 77 77
INTRINSEC SECURITE • SAS AU CAPITAL DE 2 893 420 € • SIREN : 812 535 284 • APE : 6203Z

TABLE DES MATIERES

1 INTRODUCTION

1.1 OBJET DU DOCUMENT

Ce guide est fait pour vous accompagner dans la préparation d'une gestion de crise cyber. N'hésitez pas à le lire régulièrement et à vous l'approprier. Il est accompagné d'un ensemble d'annexes nécessaires au bon déroulement de la crise, nous vous conseillons d'imprimer l'ensemble de ces documents.

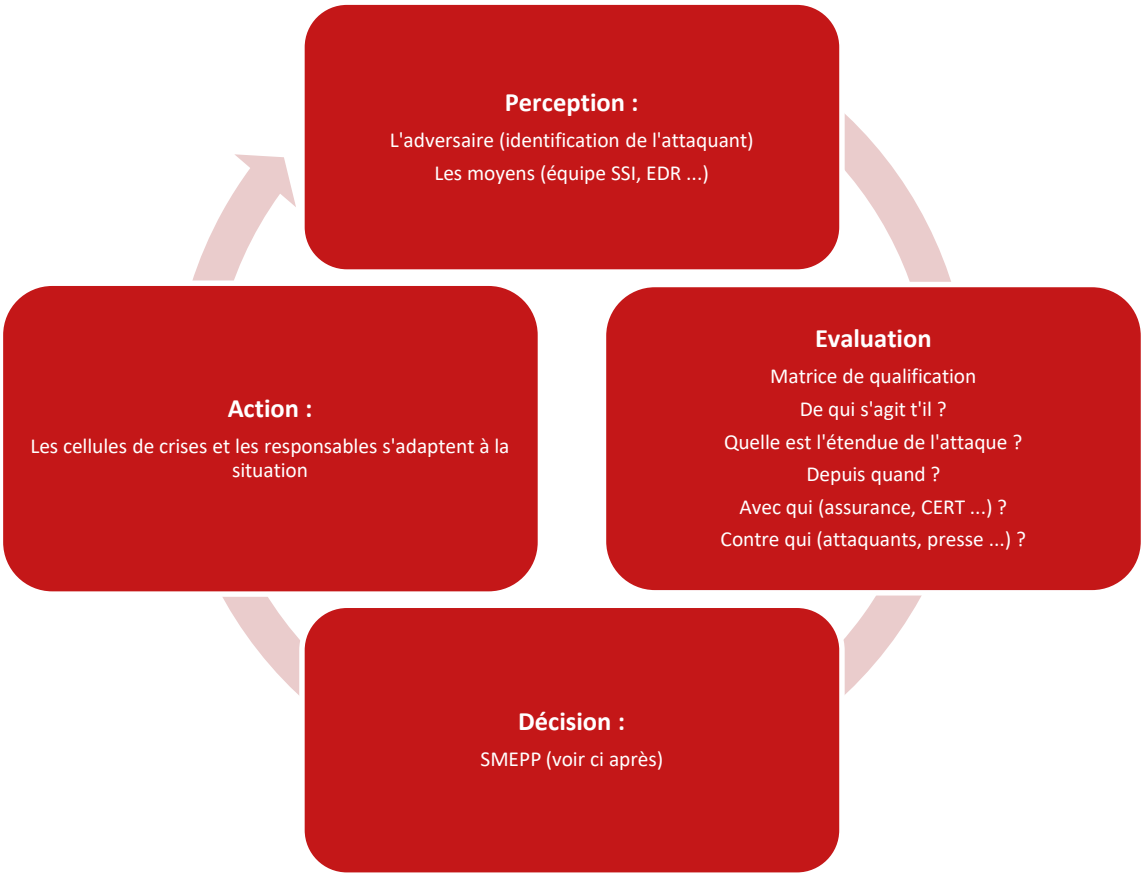
Une crise cyber est une crise majeure à cause de l'adhérence de l'entreprise au SI ; en effet, la majorité des processus, qu'ils soient de production ou de « supports » à la production, sont dépendants de l'outil informatique.

La réponse à une cyberattaque peut être assimilée à une guerre, ainsi *les principes de la guerre* (Ferdinand Foch 1903) résonnent dans l'organisation de la gestion de crise :

- **La liberté d'action :** Cette liberté commande de ne pas subir la volonté de l'adversaire mais de rester maître de son action en anticipant son mode opératoire (ex. : étude de la kill chain) et en contrecarrant ses plans (ne pas laisser l'attaquant prendre l'initiative sur la communication vers les tiers, couper ses accès au SI, limiter ses déplacements au sein du SI en isolant les systèmes infectés, …)
- **La concentration des forces :** Les moyens doivent être concentrés sur la gestion de la crise, les chantiers non prioritaires doivent être stoppés de manière à utiliser au mieux les ressources humaines et matérielles
- **L'économie des moyens :** La résolution d'une crise cyber se fait sur la durée : il faut rapidement mettre en place une organisation logistique permettant aux équipes de se reposer.

1.2 REFLEXION APPLICABLE A LA GESTION DE CRISE

Il convient de placer la gestion de crise au sein d'une boucle de réflexion nommée PEDA de manière à avoir une vision claire de l'attaque et de la situation. Cette boucle de réflexion est un outil mental mais elle peut être posée sur un tableau de manière à fournir un état des lieux visibles par tous.



1.3 SMEPP

Est considéré comme groupe au sein de la cellule de crise un ensemble de personne (ou un service) se voyant attribuer la même mission (communication, reconstruction, forensic, suivi de la main courante …).

Les missions de chaque groupe de la cellule de crise devront être définies suivant le canevas suivant :

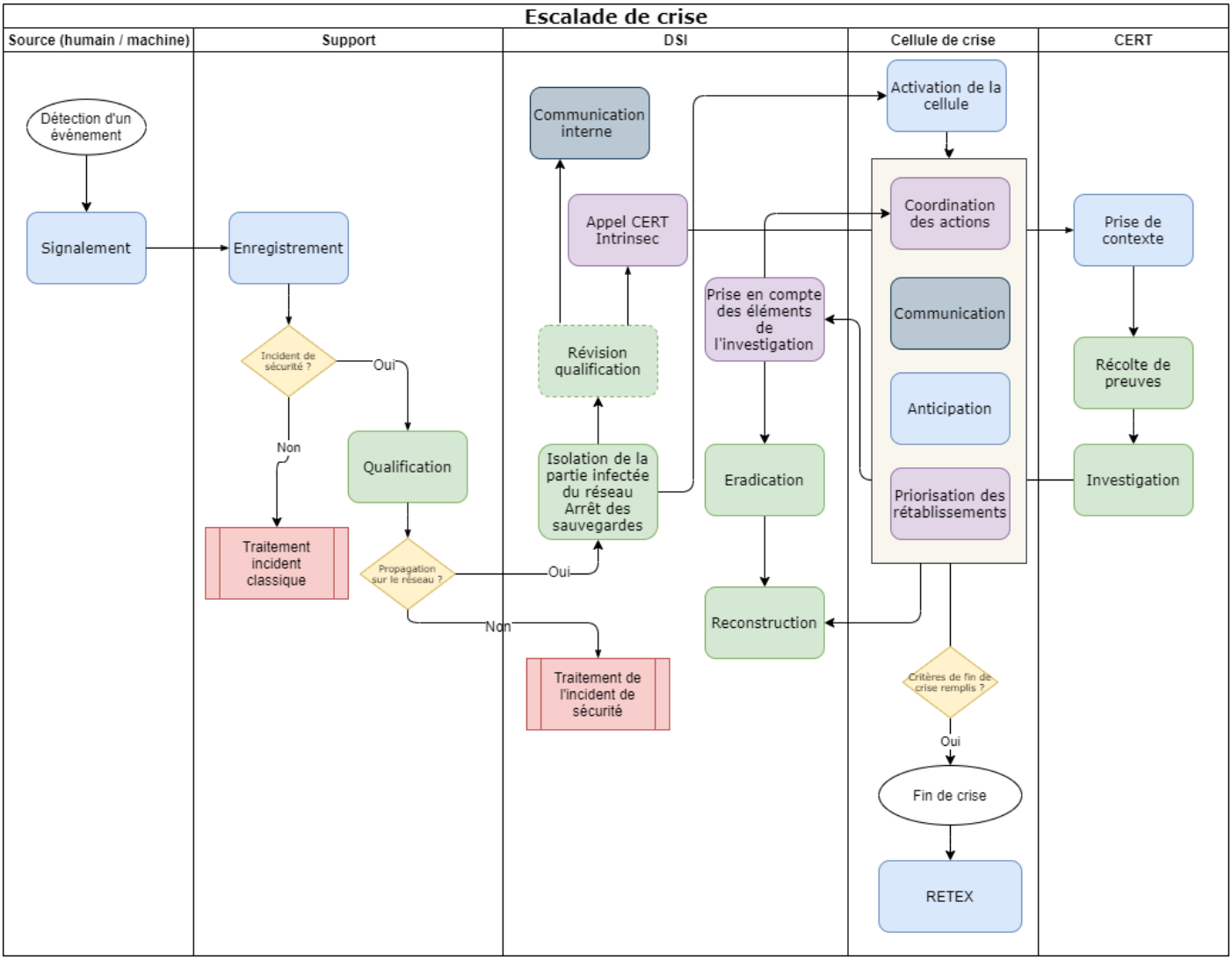
- **Situation :** Quelle est la situation générale ?
- **Mission :** Quelle est la mission donnée ?
- **Exécution :** Quelle est l'articulation au sein des groupes missionelles de la cellule de crise l'articulation peut se faire en répondant aux questions suivantes : qui fait quoi ? quels sont les moyens de communication internes/externes au groupe pour la mission?
- **Place du groupe :** Quelle est la place du groupe dans la cellule de crise, quels sont les autres groupes de la cellule de crise ?
- **Place du responsable :** Quelle est la place du responsable, de quelle cellule de crise fait-il partie, quelle est la hiérarchie pendant la crise ?

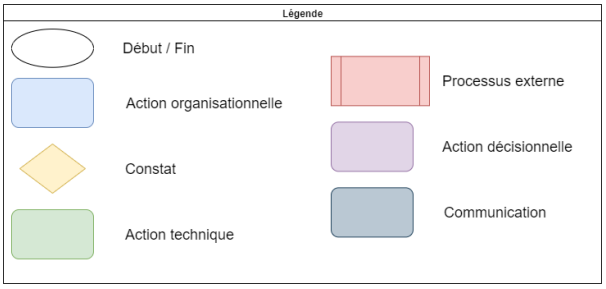
2 DISPOSITIF DE GESTION DE CRISE

2.1 PROCESSUS D'ESCALADE DE CRISE

Le processus d'escalade de crise permet de répondre efficacement à une menace de cyberattaque.

La phase d'enregistrement doit être la plus complète et la plus précise possible. La phase de qualification doit permettre la réponse la plus appropriée suivant l'incident. Cette qualification se fait au travers des fiches réflexes et des matrices de qualification.





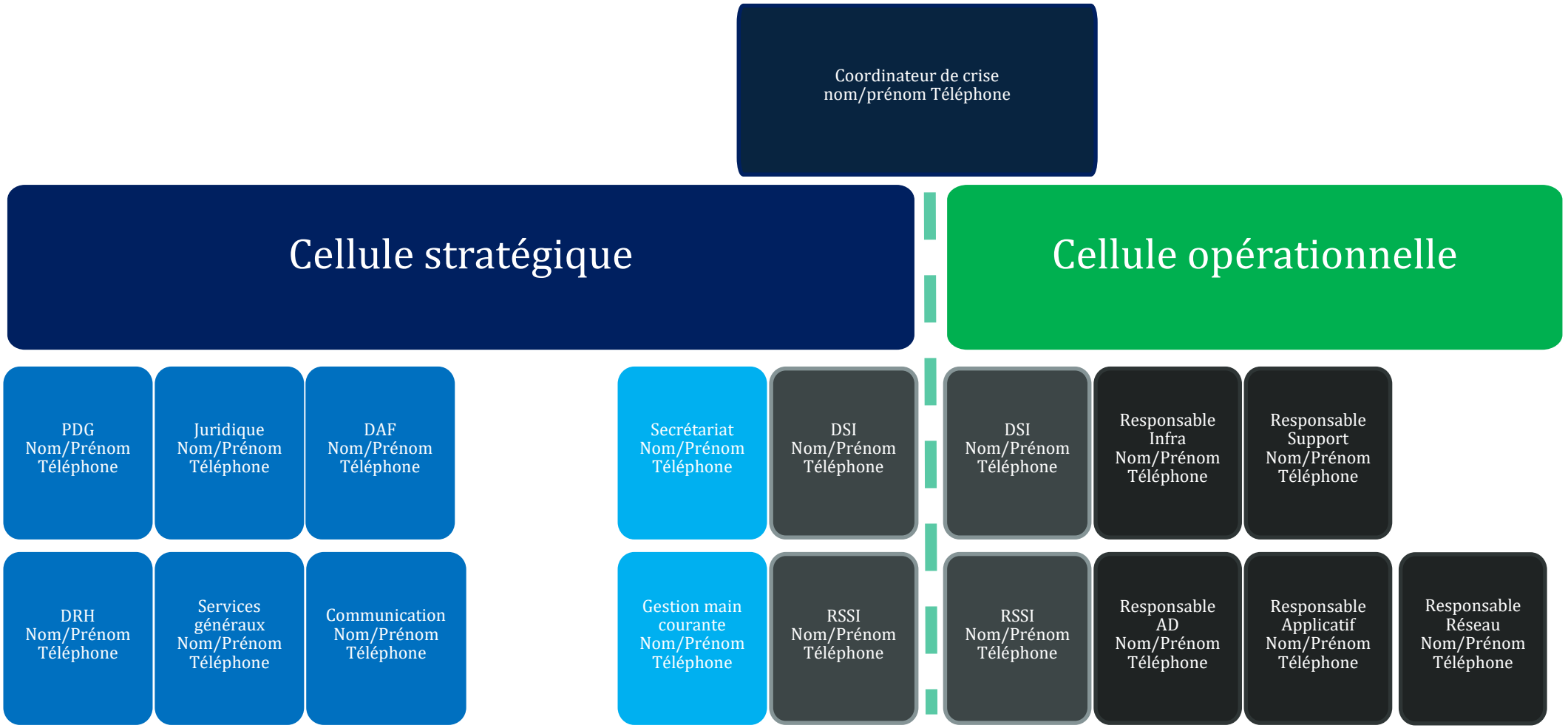
Note sur la qualification : la phase de qualification est spécifique aux crises cyber. L'étape de « révision de qualification » présentée ici au niveau DSI peut rassembler (même virtuellement, à travers un groupe dédié sur une

application de messagerie mobile sécurisée telle Signal ou Olvid), toutes les parties prenantes à même de décider / valider la qualification initiale (réalisée au niveau opérationnel / support) et s'assurer des critères d'activation des cellules de crise (les membres de ce groupe étant plus à même d'évaluer les faits observés à l'aune de la matrice des impacts)

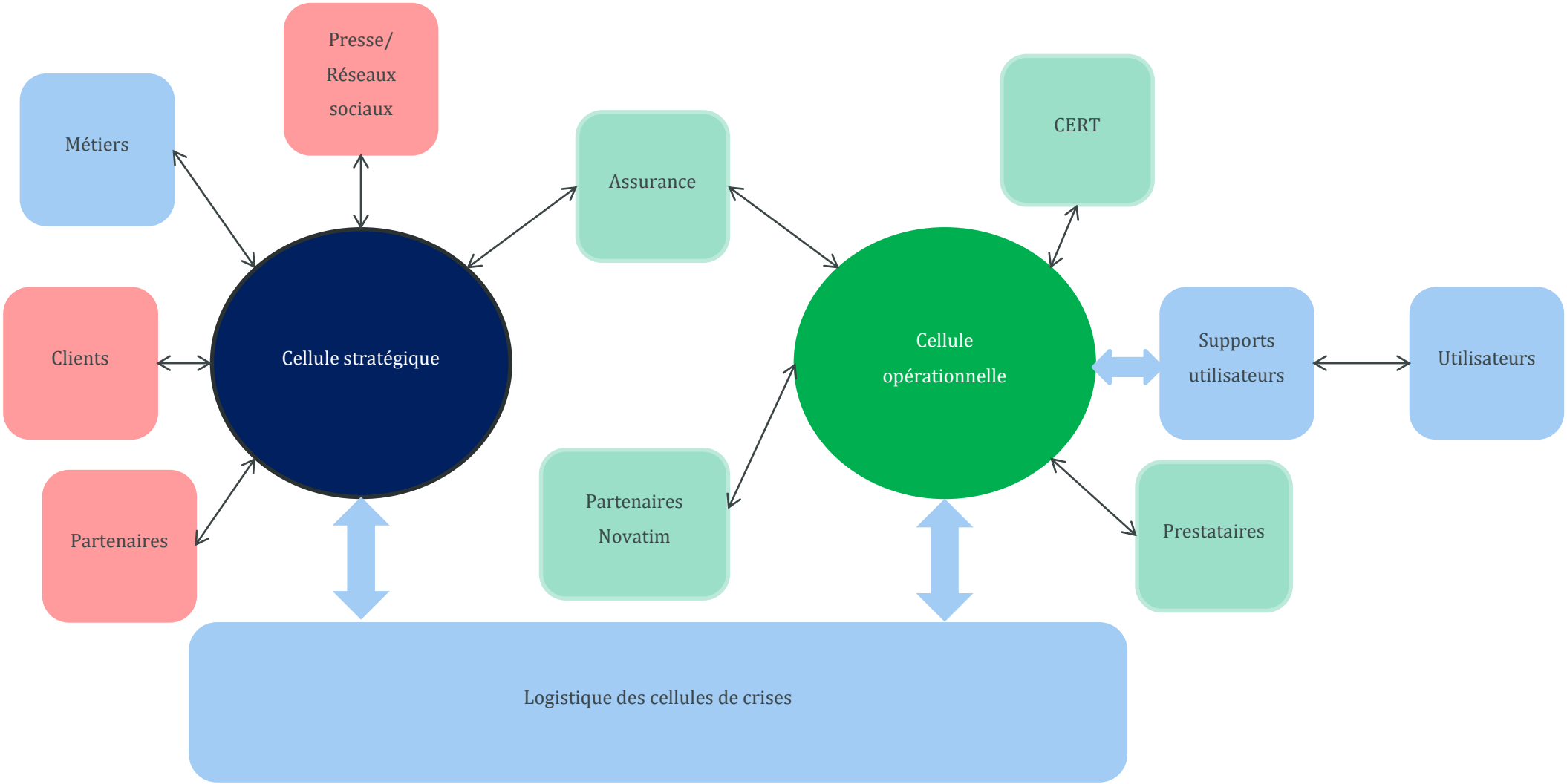
2.2 CELLULES DE CRISE

2.2.1 Répartition des cellules de crises

La répartition des cellules de crises est la suivante :



2.2.2 Interaction des cellules de crises



Les cellules de crises ont besoin de mettre en place des annuaires de crises avec les entités « amies », sources d'aide dans la crise, et « ennemies », sources de contraintes dans la crise.

Les services étatiques font également partie des forces « amies » et ont besoin d'être intégrés à l'annuaire de crise. Leurs coordonnées dépendent de la situation géographique.

2.3 LE COORDINATEUR DE CRISE

2.3.1 Missions

Le coordinateur de crise doit, après alerte par le RSSI ou le DSI :

- Alerter la direction par téléphone et par email
- Consigner les opérations techniques déjà réalisées (action, horaire) avant que les mains courantes ne soient initiées, afin que celles-ci ne se perdent pas
- Activer les cellules de crises et mobiliser leurs membres
- Répartir les missions et briefer sur la situation les cellules de crises
- Alerter les prestataires identifiés pour aider à la résolution de crise
- Contacter l'assurance cyber
- Initier la main courante

2.3.2 Outils

Pour mener à bien ses missions, il dispose des outils suivants à avoir en version papier:

- Annuaire de crise interne
- Annuaire de crise externe (prestataires, Assurance cyber…)
- Trame de main courante
- BIA (Business impact analysis présent au chapitre 2.2)
- Documentation de crise

2.4 CELLULE STRATEGIQUE

2.4.1 Missions

La cellule de crise stratégique a pour rôle le pilotage et l'organisation de la crise pour garantir une sortie de crise rapide et efficace. Elle assure une communication constante avec les partenaires extérieurs, qu'ils soient clients, prestataires, organes de presse ou autorités de l'État.

Elle décide également du moment de sortie de crise.

Dans les premiers temps de la crise, la cellule stratégique aura pour priorité d'obtenir une vision la plus claire possible des événements (qui, quoi, comment, où – et en particulier qu'est-ce qui est impacté, qui/quoi peut continuer à fonctionner et comment, et qui/quoi ne le peut pas).

Au sein de la cellule de gestion de crise stratégique nous retrouvons plusieurs missions :

2.4.1.1 *Gestion de la main courante*

La gestion de la main courante est une mission consistant à tracer l'ensemble des actions et informations en provenance et à destination de la cellule de crise. La main courante doit être mise en place dès le déclenchement de la cellule de crise et doit être clôturée lors de la décision de sortie de crise. Elle permet de justifier des actions prises auprès des partenaires et assureurs, de retracer les décisions et d'établir un retour d'expérience à la fin de la crise.

Pour aider dans cette tâche, une trame est disponible en annexe 7 de ce document.

2.4.1.2 *Communication interne*

La communication interne a pour but d'informer les collaborateurs de la situation. Cette communication doit également permettre de passer les consignes aux collaborateurs. Il est nécessaire d'adapter la communication à la cible choisie (collaborateurs, directeurs, managers de proximité).

Les thématiques principales spécifiques à la communication interne sont :

- La coordination avec les représentants du personnel dès lors que la crise impactera les conditions de travail (arrêt de travail, proposition de prise de congés avant le recours au chômage partiel, etc)
- Le versement des salaires (systèmes de gestion des paies indisponibles, obligation de rejouer la paie du mois précédent, etc..)
- Le risque de fuite de données à caractère personnel des salariés (bases RH notamment)

2.4.1.3 *Communication externe*

La communication externe a pour but d'informer les partenaires, fournisseurs et clients de la situation. Un guide de communication est disponible en annexe 2. La communication avec les clients stratégiques, ou les plus mâtures en matière de cybersécurité, devra en outre faire l'objet d'une tâche distincte (voir annexe 2 également)

2.4.1.4 *Secrétariat de crise*

Le secrétariat de crise a pour but de faire l'interface entre l'extérieur et la cellule de crise. Le secrétariat de crise doit avoir une bonne connaissance de l'entreprise. Le secrétariat de crise peut également tenir la main courante suivant le niveau de sollicitations de la cellule de crise.

2.4.1.5 *Pilotage de la crise*

Le pilotage de crise est une mission de l'ensemble de la cellule de crise stratégique. Il consiste à établir les priorités et à établir la stratégie de crise. Le pilotage ne peut être délégué uniquement au RSSI et au DSI au vu des impacts métiers.

Dans le cadre d'une intervention du CERT-Intrinsec, ce dernier pourra inclure à son dispositif un pilote de crise dédié.

2.4.2 Moyens nécessaires

Salle de crise stratégique (salle accessible 7/7 24/24) :

- 10 PC portables hors AD
- 2 box 4G avec forfait / abonnement en cours
- Nécessaire de bureau
- Tableau blanc
- Documentation de crise version papier (annuaires, main courante …)

- 10 Téléphones portables
- Eau, café, capacité de commander de la nourriture (à ajouter à l'annuaire de crise)
- Solution de communication indépendante (Signal, Teams hors tenant, mail de secours hors tenant)

2.5 CELLULE OPERATIONNELLE

2.5.1 Missions

La cellule de crise opérationnelle a pour rôle la coordination avec la cellule de crise stratégique et la prise des décisions techniques, dans le but d'apporter une sortie de crise dans les meilleures conditions. Elle assure également la coordination technique avec les partenaires éventuels d'investigation de l'incident. Elle priorise les actions techniques à effectuer en traduisant les priorités métiers définies par la cellule stratégique en systèmes IT et leurs dépendances.

Au sein de la cellule de gestion de crise opérationnelle nous retrouvons plusieurs missions :

2.5.1.1 *Confinement*

Dans le cadre d'une attaque généralisée, une coupure réseau est nécessaire. Le DSI doit être en capacité de prendre la décision de coupure, de manière à réagir au plus tôt. Selon la situation, la coupure réseau peut impacter toute la structure, ou un sous-ensemble de la structure.

La coupure réseau et la convocation de la cellule de crise sont en général concomitantes. Le DSI informe la cellule de crise de l'ampleur de l'incident et de la coupure lors de la première réunion de crise.

Quel que soit l'impact de l'attaque, il faut s'attendre également à ce que les clients coupent leurs interconnexions au réseau XXXX dès la première communication de crise.

2.5.1.2 *Collecte des preuves*

Pour mener à bien l'investigation de l'incident, qu'il soit judiciarisé ou non, des preuves doivent être collectées. Une communication régulière entre le CERT et la DSI est primordiale pour la collecte de preuves. En effet, la DSI de XXXX étant au fait de son infrastructure, la collecte sera effectuée par les équipes de la DSI, avec les outils et instructions du CERT, puis envoyées au CERT pour analyse.

2.5.1.3 *Eradication*

Il s'agit de l'éradication de l'attaquant grâce au blocage des indicateurs de compromission dans les consoles d'EDR et dans les pare-feux. Il s'agit également de la correction de la source d'intrusion.

2.5.1.4 *Reconstruction*

Il s'agit de reconstruire le SI en suivant les priorités établies par la cellule de crise stratégique et en suivant les étapes du guide présent en annexe 5.

2.5.2 Moyens nécessaires

Salle de crise opérationnelle (salle accessible 7/7 24/24) :

- 10 PC portables hors AD
- 4 box 4G avec forfait / abonnement en cours
- Nécessaire de bureau
- Tableau blanc
- Documentation de crise version papier (annuaires, main courante, cartographie réseau, cartographie applicative)
- 10 Téléphones portables
- 10 clefs USB
- Eau, café, capacité de commander de la nourriture (à ajouter à l'annuaire de crise)
- Solution de communication indépendante (Signal, Teams hors tenant, mail de secours hors tenant)
- 2 switch
- Lot de gommettes (nombre de poste * 115%)

2.6 CRITERES DE FIN DE CRISE

Il est essentiel de déterminer des critères de sortie de crise. Les services essentiels identifiés étant la production, la paie et la facturation, il paraît opportun de fixer les critères de fin de crise suivants :

- Reprise nominale des activités
- Facturation
- Paie des employés

3 ANNEXES 1 - COMMUNIQUES DE PRESSE

3.1 PLAN DE COMMUNICATION DE CRISE

3.1.1 Composition de la cellule communication

Nom prénom	Fonction	Mail secouru	TPH
	Responsable de la communication		
	Porte-parole		
	Communication externe		
	Communication interne		

3.1.2 Annuaire des médias

Journaliste		Média	Mail	TPH

3.1.3 Les TIPS de communication

- Organisez une veille des réseaux sociaux et de la presse afin d'identifier au plus tôt tout emballement médiatique
- Suspendez-les post programmé
- Donnez des instructions à la direction ainsi qu'aux élus
- N'ayez qu'une seule voix, accordez les communications en interne, envers les partenaires et la presse
- Ne cachez pas les faits, soyez transparent et communiquez rapidement sur le sujet
- Assurez-vous de communiquer des faits avérés, en accord avec la cellule de crise, le DSI, le RSSI
    - Créez une « FAQ » contenant les questions les plus courantes ou évidentes, et leurs réponses pré-validée par la cellule stratégique (avec le concours du DSI). Tout ce qui est mentionné dans cette FAQ peut être communiqué par le service de communication sans nécessiter d'approbation supplémentaire.
    - Mettez régulièrement à jour cette FAQ lors de points dédiés entre la communication et la cellule opérationnelle
- Répondez avec honnêteté et transparence, présentez des excuses sincères liées aux perturbations de service
- Corrigez les fausses informations publiées par les internautes
    - Tant que la marque n'est pas attaquée nominativement et massivement, il est inutile de chercher à répondre à toutes les mises en causes, car cela pourrait ne faire que maintenir l'événement dans les esprits et alimenter le débat. Il conviendra alors de sélectionner les prises de parole sur des critères avantageux pour l'entreprise. La qualité de la veille médiatique / réseaux sociaux permettra de décider quand répondre et quand se faire oublier

- La communication vers les **clients importants et mâtures en termes de cybersécurité** doit être traité à part (les autres pourront être intégrés à la communication externe classique).
  Le pilote de crise, assisté par la communication et la DSI doit alors établir une liste de contacts au sein des SSI de ces clients particuliers, afin de les enrôler dans une liste de diffusion présentant une à deux fois par semaine une mise à jour claire et transparente de la situation portant sur les points suivants :

  - **Investigation**
    - Date de la compromission initiale
    - Compromission initiale : quel est le vecteur initial de l'intrusion (VPN avec des comptes légitimes dérobés, fishing, etc...)
    - Date estimée de fin de l'investigation
    - Assurance de partage des indicateurs (IoC)
  - **Attaquant**
    - Nom de l'attaquant revendiqué + lien vers une source d'information crédible (exemple dans le cas de Conti : https://us-cert.cisa.gov/ncas/alerts/aa21-265a)
    - L'objectif est de donner immédiatement aux contacts sécurité de vos clients des informations actionnables
  - **Fuite de données**
    - confirmée / probable / possible / pas d'information / pas d'exfiltration
    - si confirmée ou probable :
      - Indication que vous avez mis en place une veille du site de publication de l'attaquant et de différentes sources de publication d'information sur le Dark Web (la CTI-Intrinsec aura probablement activé sa veille pour vous)
    - Promesse d'informer les clients dès une publication détectée
  - **Impacts**
    - Impact sur votre activité (quels services continuent à être rendus / quels services ne peuvent être rendus)
    - Périmètre exact de la compromission
    - Il est important ici que les clients qui ne sont pas concernés (pas sur le domaine compromis, applicatifs isolés, etc) puissent le déterminer à ce stade
    - ETA de restauration service par service (ou pas d'ETA actuellement, mais promesse de les tenir informer dans les bulletins suivants)
  - **Déclarations**
    - Confirmation d'une déclaration CNIL préliminaire, qui sera complétée en fonction de l'évolution de la situation
    - Confirmation d'un dépôt de plainte (avec numéro de la plainte) -> permet à vos clients éventuellement de se rattacher à votre plainte
  - **Renforcement de la sécurité**
    - Liste des contrôles de sécurité subis par chaque machine autorisée à revenir en ligne et chaque poste utilisateur autorisé à rejoindre le domaine
    - Nouvelles mesures de sécurité prises à ce jour (MFA sur les accès distants, extension du périmètre de l'EDR, nouveau domaine AD isolé dans un tiers 0, etc.…)
    - Toutes autres mesures de sécurité à venir (y compris processus, etc.)
  - **Propositions**
    - Offre de partage des indicateurs de compromission (IoC)
    - Offre de point 1-to-1 pour étudier les impacts de l'incident dans le cadre des interconnexions spécifiques si le bulletin ne répond pas à leurs interrogations
    - Confirmation qu'il y aura des bulletins additionnels en fonction de l'évolution des opérations de redémarrage des services

L'objectif de ce bulletin d'information régulier est d'éviter à la cellule opérationnelle d'être débordée par les sollicitations de (trop) nombreux clients attendant souvent les mêmes réponses, et de ne se mobiliser que pour les cas particuliers (interconnexions spécifiques, notamment).

Note : en cas de fuite de données avérées, les DPO des clients importants exigeront de connaître précisément la nature des données fuitées les concernant, mais aussi celles qui étaient détenues par XXXX. Dans le premier cas, la CTI-Intrinsec réalisera une analyse des données publiées par l'attaquant. Dans le second, en revanche, il reviendra aux équopes XXXX de mettre en place un atelier de recherche de données :

- Restauration dans un environnement isolé des systèmes confirmés comme étant la source des données dérobées
- Indexation de ces données à l'aide d'un outil tel File Locator Pro ()
- Demande aux DPO de fournir une liste de mots-clés souhaités (nom de l'entreprise, mais aussi implantations principales, noms de projets, etc)
- Recherche des mots-clés demandés et livraison au DPO d'un rapport exporté depuis le logiciel de recherche

Une fois mise en œuvre par la DSI sur un poste dédié, cette recherche peut être prise en charge au quotidien par un personnel administratif.

3.2 INTERNE – PREMIERE COMMUNICATION

XXX est actuellement victime d'une cyberattaque de type « Ransomware ».

Une cellule de crise a été mise en place de manière à résoudre l'incident et est en train de contacter les directeurs de services.

Les managers sont priés de :

- Mettre en place les mesures du PCA (se référer aux fiches PCA) permettant la continuité d'activité sans informatique ;
- De s'assurer de la bonne application des consignes fournies par la cellule de crise ou le service informatique.

L'ensemble des utilisateurs et des managers sont priés de :

- Signaler au XXX la présence d'une note de rançon nommée « XXX » sur leur PC ou en cas de signes de ransomware fournis par la DSI dans la fiche réflexe ci-jointe ;
- Ne pas communiquer sur l'incident en extérieur. En cas de sollicitations de la presse merci de les renvoyer vers la cellule communication de la cellule de crise joignable au « XXXXX » ;
- En cas de sollicitations des usagers, se référer aux communiqués de presse ;
- Ne sollicitez le XXX desk qu'en cas de force majeure.

Merci de votre compréhension et de votre aide dans cette situation, nous vous tiendrons informé de l'évolution de la situation.

3.3 EXTERNE – COMMUNIQUE DE PRESSE

XXX est victime d'une cyberattaque de type « Ransomware ».

Cette attaque a été détectée le XXX par les services informatiques de XXX. De manière à protéger les données de XXX, le système d'information (réseau informatique et applications) a été mis à l'arrêt. Des investigations sont en cours pour déterminer l'impact de l'attaque, à ce stade aucun vol de données n'a été identifié.

Une cellule de crise a été mise en place immédiatement par les services de XXX pour piloter la résolution de l'incident.

Cette mise à l'arrêt a des impacts forts sur nos services. Grâce à la collaboration de l'ensemble des collaborateurs de XXX nous allons mettre en place un service en mode dégradé dont les modalités vous seront transmises par nos réseaux sociaux (LISTE RSO).

XXX avec l'aide de ses partenaires et de prestataires experts en cybersécurité met tout en œuvre pour assurer un retour à la normale au plus vite.

Nous vous tiendrons informer des évolutions éventuelles et restons à votre écoute au travers du « XXXXXXXXXXX »

3.4 EXTERNE – COMMUNIQUE DE PRESSE DPO

Comme annoncé précédemment, XXX est victime d'une cyberattaque de type « Ransomware ».

Cette attaque a été détectée le XXX par les services informatiques de XXX. Les investigations menées à ce jour nous ont permis de découvrir le vol des données suivantes :

- XXX
- XXX

La CNIL (Commission nationale de l'informatique et des libertés) a été informée suivant les modalités définies par celle-ci.
Ces données pourraient être utilisées dans des campagnes de phishing à venir, nous vous invitons donc à être vigilants et à modifier vos mots de passe personnels.

Nous nous excusons des désagréments occasionnés par cette attaque et nous mettons tout en œuvre avec l'aide de nos partenaires et de nos prestataires experts en cybersécurité pour assurer un retour à la normale au plus vite.

Nous continuerons de vous tenir informer des évolutions de cette attaque et restons à votre écoute au travers du « XXXXXXXXXXX »

4 ANNEXE 2 - GUIDE DE RECONSTRUCTION

4.1 PRINCIPES GENERAUX

Ces principes directeurs guideront les travaux de reconstruction du SI post-incident. Ils doivent être adaptés en fonction des éléments remontés par l'investigation, notamment en ce qui concerne le niveau technique observé de l'attaquant et son emprise sur le système d'information.

Il sera important de disposer de plusieurs zones réseau isolées au niveau du pare-feu :

1. **Zone compromise** : La zone « rouge » est le SI compromis (ou le périmètre compromis au sein du SI global, si ce dernier était segmenté). Toute machine présente sur ce périmètre, quel que soit son état réel, doit être considérée comme compromise et devra suivre le processus de remédiation.

2. **Zone d'attente** : Dans un processus impliquant plusieurs équipes travaillant en parallèle à la remédiation, la zone d'attente permet de stocker les machines éteintes (VMs) devant être remédié. Elle permet la priorisation des machines par l'équipe DSI : seules les machines présentes dans cette zone peuvent être récupérées par les équipes de remédiation pour traitement.

3. **Zone de reconstruction** : La zone « grise » reçoit les machines restaurées depuis les backups ou récupérées depuis le SI compromis et déposées éteintes dans la zone d'attente. Il s'agit d'une zone de travail, et les machines n'ont pas vocation à y demeurer ou à s'y croiser. Chaque machine en cours de traitement est seule dans cette zone, et s'il est nécessaire de paralléliser, cela devra se faire par la multiplication des zones grises (une par équipe de reconstruction). La zone de restauration de l'AD est prête et opérationnelle.

4. **Zone de confiance** : La zone « verte » est celle où sont remises en service les machines de production. Il s'agit du SI-cible, celui sur lequel l'activité reprendra.
   Elle ne doit avoir aucun contact avec d'autres zones que les zones grises de reconstruction. Seule exception : dans le cadre d'une procédure de restauration « en place », les machines remédiées sont progressivement déposées éteintes dans le SI d'origine (la zone rouge qui, de fait, se verdit progressivement), tandis que celui demeure à l'arrêt jusqu'au verdissement complet.

Ces différentes zones permettront de créer un flux industrialisé de restauration des machines dans de bonnes conditions de sécurité, après avoir subi les contrôles adéquats.

Mais avant de lancer un tel processus de remédiation, il est nécessaire de pouvoir s'appuyer sur un annuaire Active Directory **isolé** et **de confiance**, afin de soutenir l'ensemble des services d'infrastructure nécessaires au redémarrage.

Cette étape peut être anticipée et commencer dès le début de la réponse à incident, car elle ne dépend pas d'indicateurs de compromission fournis par l'investigation**, contrairement aux opérations de restauration des machines**.

Les services Cloud ne font pas partie des périmètres de reconstruction, néanmoins par principe de précautions il faut changer l'ensemble des credentials et forcer le MFA.

L'attaquant ayant pu intercepter des tickets il est nécessaire de changer les tickets et de vérifier les changements de comptes ou de configurations sur ces services.

Dès que les postes sont considérés comme sain, les flux peuvent être réouverts entre les postes et les services Cloud.

4.2 TRAVAUX PREPARATOIRES

Tandis que l'investigation numérique démarre, il est possible de préparer une partie du SI afin d'anticiper sur les opérations à venir.

4.2.1 Création d'une bulle de confiance

Il est important de repartir sur un Active Directory de confiance, placé dans un VLAN neuf, isolé du reste de l'infrastructure par un filtrage en sortie de VLAN (**deny all, all** initialement). Cette zone de confiance ne deviendra pas nécessairement le SI-Cible à terme (bien qu'elle soit souvent ensuite pérennisée dans son rôle de VLAN tiers 0 pour les actifs critiques), mais elle permettra de remonter des services d'infrastructure qui soutiendront les opérations futures.

- Ce VLAN ne doit être accédé que depuis des postes de travail neufs (réimagés) et isolés pour la réinstallation.
- Ce VLAN doit recevoir à minima une VM Windows neuve en version récente (le dernier niveau de version acceptable) destinée à devenir le nouveau contrôleur de domaine primaire

4.2.2 Création du futur contrôleur de domaine primaire

Le principe de création du futur contrôleur de domaine primaire consiste en une double réplication : à partir d'un DC dont l'état ne peut être assuré (perte de confiance dans le système Windows et dans la structure AD), une première réplication vers une VM neuve permet de regagner la confiance dans le système Windows (mais toujours pas dans la structure AD). Sur ce DC intermédiaire, des opérations de contrôle et de nettoyage de la structure AD viendront préparer la dernière synchronisation vers le DC final (isolé au sein de la bulle de confiance), ce qui permettra alors de retrouver la confiance tant dans son système Windows que dans sa structure AD.

Procédure :

- La VM Windows présente dans la bulle de confiance (cf étapes précédentes) doit être configurée comme un DC prêt à être synchronisé avec un DC existant, avant d'être promu. **Elle doit demeurer parfaitement isolée de toute autre zone durant l'intégralité de cette procédure**.
- Sur une zone neutre (pas sur le SI compromis) créer un second DC vierge identique à celui présent dans la bulle de confiance. Ce sera **le DC intermédiaire**.
- Identifier un DC existant (potentiellement compromis), ou en récupérer un depuis les backups à la date la plus ancienne acceptable (à ce stade l'investigation numérique n'a pas fourni de date d'intrusion initiale qui

permettrait d'avoir l'assurance de récupérer une image d'un DC sain)

- Autoriser le DC intermédiaire à se synchroniser avec le DC compromis

4.2.3 Nettoyage de la structure AD

Une fois le DC intermédiaire synchronisé, il est nécessaire de nettoyer sa structure AD.

Il est considéré impossible de *réellement* nettoyer un AD complexe compromis. La seule solution de confiance est la reconstruction. Toutefois, cela est rarement possible dans des conditions réelles d'intervention et les exigences de reprise d'activité. Il est alors nécessaire d'accepter le risque de repartir sur un AD *partiellement* nettoyé.

Procédure de nettoyage :

- Revue des comptes afin d'identifier, valider et supprimer l'ensemble des créations / modifications de comptes ou droits privilégiés (outil ADrecon : https://github.com/sense-of-security/ADRecon)

- Audit des GPO (présence de politiques malveillantes qui peuvent pousser des codes malveillants ou des tâches programmées sur les postes)

Il est important à ce stade d'être en mesure d'identifier et supprimer les comptes qui ont pu être créés ou modifiés (ajout de droit, ajout à des groupes…) par l'attaquant. Seule une très bonne connaissance de l'AD par les équipes opérationnelles permettra d'être efficace ici.

4.2.4 Synchronisation du PDC

Le PDC dans la bulle de confiance est prêt à être synchronisé avec le DC intermédiaire nettoyé.

Pour cela, seuls les flux nécessaires à la réplication doivent être ouverts sur le pare-feu, et uniquement entre les IP des deux machines.

4.2.5 Reset des secrets

Une fois le PDC disponible dans la bulle de confiance, il est nécessaire de changer l'ensemble de ses secrets :

- Comptes utilisateurs
- Comptes de service
- Compte KRBTGT (Microsoft propose des scripts pour cela : https://www.microsoft.com/security/blog/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/)

4.2.5.1 *Cas particulier d'ADFS / ADconnect*

Dans le cas de services dans le Cloud public dont l'accès est adossé à l'AD *on-premises*, une fois le SI à l'arrêt, les jetons d'authentification des actifs Cloud resteront valides et ne pourront pas être renouvelés tant que le nouvel AD

ne sera opérationnel. Dans cet intervalle (qui peut durer plusieurs jours), un attaquant ayant exfiltré la base utilisateur NTDS de l'Active Directory *pourrait* être en mesure de procéder à une attaque par force brute hors-ligne afin de tenter des authentifications depuis l'Internet public vers les actifs Cloud.

Il peut être alors tentant de couper le lien et rendre les services Cloud publics autonomes grâce à AzureAD (sur la base d'une population limitée), mais en pratique cela s'est souvent révélé un projet complexe et chronophage, et il a été jugé plus efficace de mettre l'accent sur une remontée plus rapide de l'AD *on-premises.*

Des tests préalables des deux scénarios dans le contexte de l'entreprise pourraient aider à choisir la bonne option le moment venu.

4.2.6 Durcissement de l'AD

Si le temps de reconstruction le permet, cet AD devra répondre au niveau 3 des recommandations AD de l'ANSSI : https://www.cert.ssi.gouv.fr/uploads/guide-ad.html

En temps contraint, il sera malgré tout important de s'assurer **qu'aucune alerte de niveau 1 ne subsiste** avant la remise en production, et d'évoluer vers le niveau 3 progressivement ensuite.

4.2.7 Ajout de services critiques à la bulle de confiance

D'autres services critiques peuvent être déployés au sein de la bulle de confiance. Dans l'idéal, il s'agit de services d'infrastructure dont la compromission pourrait permettre à l'attaquant de contrôler totalement le SI (WSUS, consoles d'outils de sécurité, etc.). Aucun service de production ne devrait rejoindre la bulle de confiance.

Chaque service intégré à la bulle de confiance devra être soit réinstallé *from scratch* ou depuis des backups bien antérieurs à l'attaque (date de première intrusion fournie par le CERT), soit avoir suivi la procédure de contrôle présentée plus loin. Cependant, la première option est largement préférable.

À chaque nouveau service ajouté à la bulle de confiance, seulement les flux strictement nécessaires à son bon fonctionnement doivent être ouverts (source, destination, ports). Cette ouverture progressive est le gage d'une maîtrise accrue de vos risques : en partant d'une règle de fermeture totale, il devient possible de maîtriser totalement (et progressivement) qui parle avec quoi et pourquoi. Cela permettra de limiter à l'avenir la capacité de reconnaissance et de déplacement d'un attaquant éventuel.

Il est conseillé de consigner ces règles dans une matrice des flux (un Excel le plus souvent) afin d'en garder la trace pour validation. Des solutions commerciales existent pour faciliter ce suivi : Tufin, AlgoSec ou Firemon par exemple – bien qu'il ne s'agisse pas ici d'une recommandation officielle de la société Intrinsec.

C'est un travail fastidieux et chronophage, mais qui paiera à terme - et la sortie de crise est le bon moment pour le faire ! Par la suite, en période de run, cette matrice des flux devra être maintenue, ce qui peut alourdir les processus d'ouverture de flux pour les métiers. Mais il s'agit d'un gage de contrôle et de sécurité.

4.3 OPTIONS / OPPORTUNITES

4.3.1 Segmentation réseau

Dans l'approche présentée jusqu'ici, la bulle de confiance ainsi créée n'héberge que l'annuaire Active Directory. Mais la crise peut être l'opportunité de renforcer la résilience du SI en le segmentant, en profitant de sa mise à l'arrêt.

Ainsi, en fonction des choix de reconstructions (très dépendants des ressources disponibles et du temps d'arrêt accepté), la bulle de confiance peut demeurer telle quelle (et devenir alors le réseau d'administration de l'AD), ou bien recevoir d'autres services d'infrastructure critiques (voir ci-dessus) ou même encore servir de point de départ à un vrai projet de segmentation réseau, basé sur trois tiers de criticité :

- Tiers0 : l'AD et les services d'infrastructure critiques
- Tiers1 : Les applicatifs métiers et de support (serveurs de fichiers, d'impression, etc.)
- Tiers2 : Les postes utilisateurs

Les administrateurs ne devraient avoir accès qu'aux tiers pour lesquels ils sont réellement administrateurs (notamment, un administrateur de tiers0 ne devrait pas pouvoir se connecter à autre chose que des machines dans le VLAN tiers0).

- Spécifiquement pour le tiers0, l'idéal est de dédier des PC à ces tâches d'administration - ou au moins avoir une VM dédiée.
    - Cette distinction peut se faire via des GPO

Quelques points de vérification peuvent être proposés afin d'évaluer l'isolation entre les tiers ou au sein de chaque tiers :

- Un poste utilisateur (tiers2) ne devrait pas être en mesure de faire du RDP sur un DC (tiers0), par exemple

- Les postes utilisateurs ne devraient pas être en mesure de se voir entre eux au sein du tiers2 (sauf exigence métier forte, il est rare aujourd'hui que des postes de travail aient besoin de fournir des services réseau à d'autres postes de travail, tels le partage de fichiers ou l'impression). Les postes de travail (tiers2) ne devraient donc pouvoir n'accéder qu'aux services fournis par des actifs en tiers1 sur des ports spécifiques, et non se voir entre eux

4.4 PROCEDURE DE RECONSTRUCTION/REMEDIATION

Pour démarrer, la reconstruction/remédiation devra disposer de deux éléments fournis par le CERT :

- La date d'intrusion initiale
- Un jeu de marqueurs de compromission stables (bien que non exhaustifs et évolutifs)

Les zones de confiances peuvent êtres démarré en parallèle sans attendre ces éléments.

4.4.1 Serveurs

Les serveurs doivent être reconstruit suivant les priorités établies dans l'annexe 5.

La procédure de remédiation pour le parc serveur est la suivante :

- Extraction des VMs à restaurer selon les priorités définies par la cellule de crise managériale et traduites en machines & dépendances par la cellule de crise technique
    - Depuis le SI compromis si pas de backup disponible
    - Depuis les backups si disponibles
        - À une date antérieure à la date de compromission initiale si possible

- Dépôt des VMs dans la zone tampon, étiquetées avec leur ordre de traitement souhaité

- Déplacement par les équipes de remédiation dans une zone « grise » de traitement.

Au sein de chaque zone de traitement (si plusieurs équipes travaillent en parallèle) :

- Démarrage de la VM
    - Si elle ne démarre pas -> réinstallation

- Passage de l'outil FastFind fourni par le CERT afin d'identifier les marqueurs connus à ce jour
    - Si correspondance, la machine doit être isolée, le CERT alerté et la VM doit être conservée à disposition du CERT si un prélèvement complémentaire de traces est nécessaire

- Installation du client antivirus à jour avec signature *custom* fournie par l'éditeur intégrant les marqueurs identifiés par le CERT

- Mise à jour à la dernière version de Windows

- Toute autre action de configuration / renforcement de la sécurité nécessaire (installation du client EDR, etc.)

- Extinction de la machine et ajout d'un tag « Vert ».

- Déplacement de la VM éteinte dans le SI – cible (nouveau VLAN ou SI historique)

À ce stade, les VMs présentes dans le SI-cible pourront être rallumées en fonction des priorités et des choix de l'équipe de pilotage et de la DSI.

4.4.1.1 *Récupération de données uniquement sur une machine infectée*

Dans le cas des machines issues de backups postérieurs à la date de première intrusion, il est préférable de favoriser la récupération sélective de données plutôt que de récupérer l'ensemble de la VM (extraction des données demandées par le métier depuis partition « data » et réinstallation sur une VM neuve).

Dans ce cas, les données récupérées devront être blanchies à l'aide d'un scan antivirus, par une inspection visuelle, ou toute autre analyse jugée satisfaisante. Le risque n'est plus celui d'un système Windows compromis, mais de documents (MS Office, PDF, etc.) piégés.

Ce type de récupération est toutefois plus long, et ne devrait être réservé qu'aux demandes critiques des métiers, pour des données dont la fraîcheur est capitale.

4.4.2 **Postes de travail**

Bien que les postes de travail soient *aujourd'hui* rarement piégés dans le cadre d'une attaque de type de ransomware, cela ne peut être exclu (c'est une évolution probable). Il est donc nécessaire de considérer que tout poste joint au domaine compromis sur la période de l'attaque est compromis. La totalité du parc utilisateur concerné doit donc être traitée, même si seule une partie de celui-ci a probablement été impactée ou présente des artefacts visibles (note de rançon, extensions du chiffreur, etc.)

En fonction des contraintes logistiques et de la nature des postes, il est nécessaire de préparer une organisation capable de :

- S'assurer qu'un poste non contrôlé ne pourra se reconnecter au réseau une fois celui-ci rallumé (filtrage par adresse MAC par exemple)

- Collecter les postes :
    - Soit les récupérer auprès des utilisateurs et les stocker (en central ou de manière distribuée en s'appuyant sur une organisation décentralisée au sein des filiales et des bureaux)
    - Soit en organisant des passages pour les utilisateurs à des points de vérification / réinstallation installés dans les différentes implantations

- Valider les postes :
    - La procédure est la même que pour les VMs serveur plus haut
    - Et l'on peut en profiter pour déployer un outil de prise de contrôle à distance ou déployer l'EDR

- Rejoindre le poste au domaine et changer le mot de passe d'administrateur local (c'est une bonne occasion de revoir cette politique)

- Marquer le poste (pastille autocollante verte par exemple) et renseigner un outil de suivi de la remédiation des postes utilisateurs (document Excel, feuille de calcul partagée, outil en ligne…)

Il est critique de pouvoir assurer la traçabilité de la remédiation des postes :

- Afin de s'assurer qu'un poste compromis ne puisse rejoindre le nouveau domaine
- Afin de pouvoir répondre aux questions / exigences des clients et partenaires qui souhaiteront connaître les contrôles appliqués aux postes et si ceux susceptibles d'intervenir chez eux ont été validés

4.5 SUIVI DES OPERATIONS DE REMEDIATION

La progression des opérations de remédiation doit être suivie et documentée à minima selon les étapes et les métriques suivantes :

- Disponibilité du VLAN de la bulle de confiance
- Disponibilité des VMs Windows vierges (nouvel AD, DC temporaire…)
- Disponibilité de l'AD vierge (bulle de confiance) et de l'AD temporaire
- Disponibilité du DC source (compromis) pour réplication vers l'AD temporaire
- Disponibilité des diverses zones de travail
- Début de la remédiation serveur
    - Nombre total de machines
    - Nombre de machines identifiées pour les procédures de restauration / contrôle
    - Nombre de machines en attente dans la zone tampon
    - Nombre de machines en cours de traitement
    - Nombre de machines compromises à reconstruire
    - Nombres et nature des machines traitées et disponibles pour rallumage
- Début de la collecte des postes de travail
    - Nombre de postes de travail collectés
    - Nombre de postes de travail traités
    - Nombre de postes de travail compromis
    - Nombre de postes de travail reconnectés au nouveau domaine

En parallèle, un suivi de la remontée des applications métiers et de leurs dépendances devra être réalisé quotidiennement afin d'alimenter la prise de décision et la réévaluation des priorités par la cellule de crise managériale.

4.6 RENFORCEMENT DES ACCES DISTANTS

La décision de réouverture des accès distants doit faire l'objet d'une discussion formelle au sein des cellules de crise.

Dans tous les cas, avant réouverture de l'accès Internet :

- L'ensemble des secrets VPN (comptes de tous les utilisateurs et certificats) doit être renouvelé

- Les certificats des tunnels IPSEC doivent être renouvelé et les matrice de flux doivent respecter le principe de moindre privilèges

- Il est vital de déployer au plus vite du MFA sur l'ensemble des points d'accès distants exposés à Internet (une fois que ceux-ci seront identifiés et remis en service)

- L'ensemble des mots de passe des éléments d'infrastructures (backbone, switch,firewall,…) doivent être renouvelés par des mots de passes nouveaux, complexes et uniques.

4.7 REOUVERTURE DES ACCES INTERNET

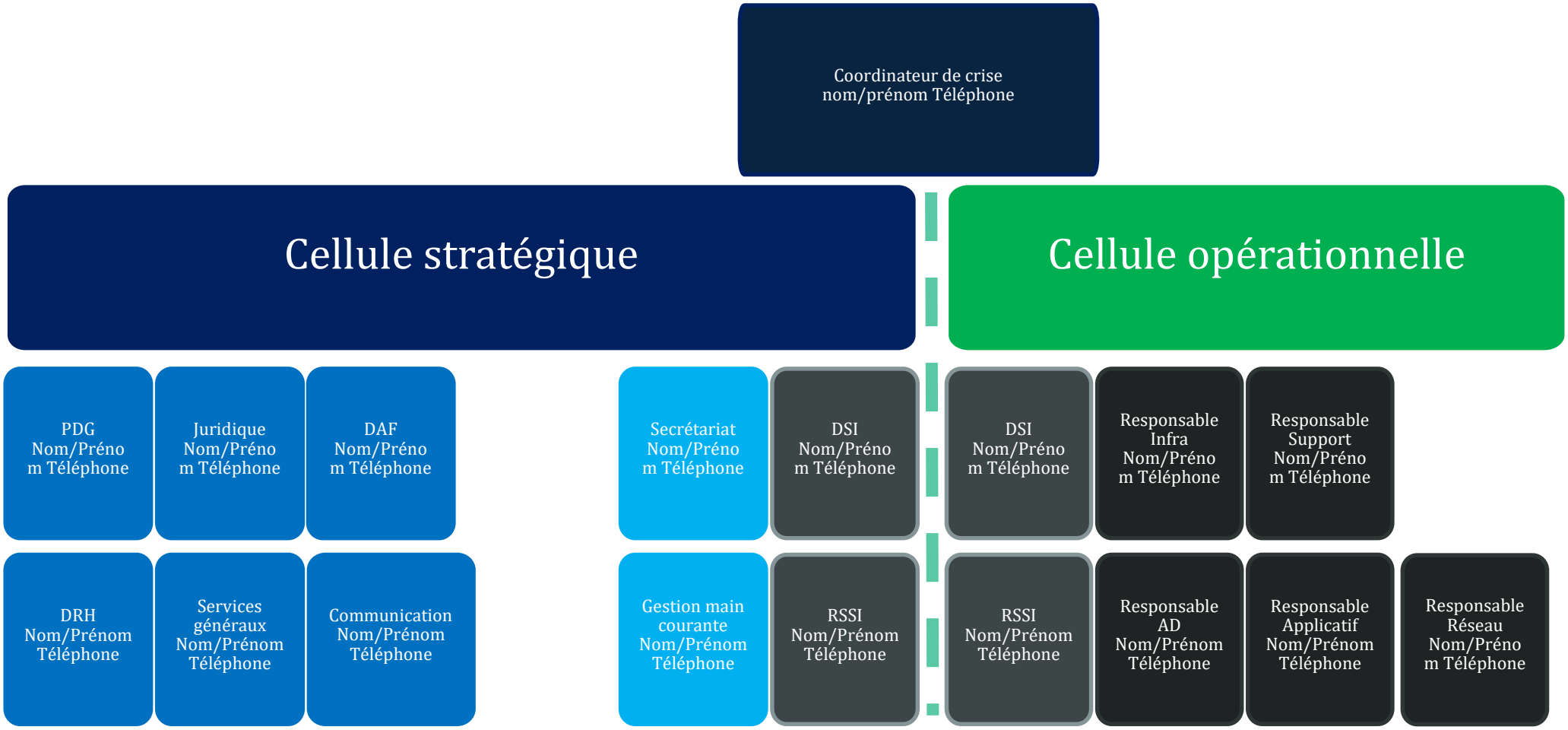
La réouverture des accès Internet est un moment clé : si l'on ne s'est pas assuré de l'absence de persistance sur l'ensemble du SI, l'attaquant peut être en mesure de reprendre le contrôle. Nous suggérons de se coordonner avec le CERT-Intrinsec avant toute décision de réouverture de l'accès Internet.

Par ailleurs, nous conseillons de ne rouvrir que les accès essentiels dans un premier temps, par un filtrage au niveau du pare-feu (0365, applications métiers SaaS, mises à jour antivirus ou EDR, etc.). Ceux-ci permettent de reprendre l'activité à minima tout en prenant le temps de superviser l'accès et de ne rouvrir plus largement (à la navigation web) qu'une fois que l'essentiel fonctionnel.

Une fois l'accès rouvert, nous conseillons une campagne de scan externe sur votre périmètre (toutes vos plages IP et vos domaines) afin d'identifier d'éventuels oublis (RDP ouvert, NAS visibles par erreur, listing de répertoire laissé ouvert sur un serveur web, etc.)

5 ANNEXE 3 – ANNUAIRES

5.1 ANNUAIRE INTERNE



5.2 Annuaire Prestataires

Nom et type du prestataire	Fonction	Nom/Prénom	Tél.
	Cyberassurances		

5.3 Annuaire Representants de l'etat

Organisation	Nom/Prénom	Tél. ou mail
Correspondant régional ANSSI	Patrice BIGEARD / Renaud ECHARD	Ile-de-france@ssi.gouv.fr
BEFTI (Ile de france uniquement)		Passer par le commissariat
CERT-FR		+33 (0)1 71 75 84 68

TOUR CBX, 20ème ETAGE, 1 PASSERELLE DES REFLETS, 92913 PARIS LA DEFENSE CEDEX • TEL +33 1 41 91 77 77
INTRINSEC SECURITE • SAS AU CAPITAL DE 2 893 420 € • SIREN : 812 535 284 • APE : 6203Z

6 ANNEXE 4 - TRAME DE MAIN COURANTE

Date	Heure demande	Heure début	Heure fin	demande	type	responsable	statut	Remarque