Procédure de Gestion des Incidents de Sécurité

– *AgroRand*

Faite Par :

Anis OUERSIGHNI

Contexte et objectifs

AgroRand est une PME technologique (environ 90 employés répartis entre le siège de Mâcon et des télétravailleurs) spécialisée dans la gestion autonome de drones IoT et le traitement cloud de données. Ses actifs critiques incluent des serveurs cloud, des drones IoT déployés sur le terrain, un CRM SaaS, un ERP local au siège, ainsi que des outils de communication interne. Une analyse des risques a mis en évidence plusieurs menaces majeures : fuite de données sensibles, ransomware (rançongiciel), campagnes de phishing ciblant les employés, exploitation de failles sur des systèmes non mis à jour, etc. Ces scénarios d'incident pourraient gravement impacter l'activité d'AgroRand (perte ou divulgation de données, interruption de service, atteinte à l'image, coûts financiers).

Conformément aux bonnes pratiques de l'ANSSI, en particulier la règle 40 du guide d'hygiène informatique recommandant de **définir une procédure de gestion des incidents de sécurité** : la société AgroRand formalise ci-dessous sa procédure de réponse aux incidents. L'objectif est de détecter et traiter rapidement tout incident afin d'en minimiser l'impact, de rétablir le fonctionnement normal des systèmes critiques, et d'en tirer des enseignements pour renforcer à terme la sécurité. Ce document, rédigé pour une lecture opérationnelle, décrit les phases clés de la gestion d'incident (détection, qualification, confinement, éradication, récupération, communication, journalisation, retour d'expérience) en précisant les rôles de chacun et les outils mobilisés à chaque étape.

Rôles et responsabilités

Une réponse efficace aux incidents repose sur une clarification des acteurs impliqués :

- **Responsable Sécurité IT (RSI)** – Il pilote la gestion de l'incident. Référent sécurité de l'entreprise (connu de tous les employés), il coordonne les actions de réponse du début à la fin. **Il** qualifie l'incident, mobilise les ressources nécessaires (internes ou externes), prend les décisions techniques et organisationnelles pour contenir la menace, et assure la communication auprès de la direction et, si besoin, vers l'externe. Il veille également à la bonne journalisation de l'incident et supervise le retour d'expérience.

- **Administrateurs Systèmes & Réseaux** – Ils mettent en œuvre les mesures techniques de protection et de rétablissement. *En phase de confinement,* ils isolent les systèmes compromis (déconnexion réseau, blocage d'accès, segmentation), appliquent les correctifs ou changements de configuration urgents, et réalisent les sauvegardes d'urgence des données et journaux. *En phase d'éradication/récupération*, ils nettoient ou réinstallent les machines infectées, restaurent les données depuis les sauvegardes et s'assurent du bon fonctionnement des systèmes remis en production.

- **Développeurs (équipes applicatives)** – Ils apportent leur expertise sur les applications et services cloud développés en interne. *Si l'incident provient d'une vulnérabilité applicative ou d'un dysfonctionnement logiciel*, ils analysent la faille et développent un correctif. Ils peuvent aider à comprendre l'ampleur de l'incident (ex : quelles données ont pu être exposées depuis le cloud) et à remettre en service les applications impactées une fois la menace éliminée.

- **Ingénieurs terrain (drones IoT)** – Responsables des drones et capteurs IoT déployés, ils interviennent si un incident affecte ces dispositifs. Par exemple, en cas de suspicion de compromission d'un drone (intrusion, détournement), ils peuvent isoler l'appareil (désactivation à distance, récupération physique), appliquer des mises à jour de firmware de sécurité, ou segmenter le réseau IoT en collaboration avec Administrateur Systèmes et Réseaux. Ils fournissent également au RSI les informations techniques spécifiques sur le fonctionnement des drones pour aider à la qualification et à l'éradication de la menace.

- **Utilisateurs (employés)** – Tous les salariés d'AgroRand ont un rôle de ***sentinelle***. Ils doivent rester vigilants et **signaler immédiatement tout incident ou activité anormale** (email de phishing suspect, fichiers chiffrés subitement, appareil égaré, etc.) **au point de contact défini** (le RSI ou la cellule IT dédiée) [Règle 38 du guide]. Ils appliquent les consignes de sécurité émises (par exemple déconnecter un poste dès qu'une infection ransomware est suspectée, changer un mot de passe compromis, etc.) et coopèrent aux enquêtes (fournir des informations, ne pas effacer de données liées à l'incident). Leur proactivité est essentielle pour une détection rapide et une réaction immédiate.

Outils de sécurité et moyens techniques

Agro Rand s'appuie sur un ensemble d'outils que nous avons implémenté lors de notre projet et qui sont vitaux pour la détection , qualification et traitement des incidents. Ces mesures inclus :

1. **EDR (Endpoint Detection & Response)** – Agents déployés sur les postes de travail des employés et les serveurs critiques. L'EDR supervise en continu l'activité des endpoints et remonte des alertes en cas de comportement suspect (ex : exécution d'un logiciel malveillant, modifications système typiques d'un ransomware). Il peut bloquer ou isoler automatiquement un poste compromis du réseau.

2. **DLP (Data Loss Prevention)** – Solutions de prévention des fuites de données installées sur les postes et sur la passerelle Internet. Le DLP surveille les flux de données sortants (emails, transferts de fichiers, USB) et déclenche des alertes en cas d'envoi non autorisé de données sensibles (ex : vol de bases de clients). Cela permet de détecter rapidement une exfiltration de données et de la stopper avant qu'elle n'aboutisse.

3. **Supervision centralisée (SIEM & journalisation)** – AgroRand collecte et centralise les journaux des systèmes critiques (serveurs cloud, ERP, réseau, drones IoT) dans un SIEM. Des règles de corrélation et des alertes sont définies pour repérer des *patterns* d'incident (tentatives d'intrusion, anomalies de connexion, etc.). Cette supervision fournit une visibilité en temps réel sur le SI et alerte le RSI en cas d'événement anormal. *(Conformément à l'hygiène ANSSI, les composants importants génèrent des journaux de sécurité complets, règle 36 .)*

4. **Segmentation réseau** – Le réseau interne est segmenté en zones de sécurité distinctes (par exemple : réseau bureautique des utilisateurs, réseau des drones/IoT, réseau serveurs sensibles (stockage), DMZ pour services exposés). Des pare-feu et règles de filtrage limitent les communications entre ces segments au strict nécessaire. En cas d'incident sur une zone (par ex. poste utilisateur infecté), la segmentation ralentit voire empêche la propagation au reste du SI, facilitant le confinement.

5. **Authentification multi-facteur (MFA)** – Tous les accès aux services critiques (des télétravailleurs qui veulent accéder par ssh aux postes, accès administrateur aux serveurs cloud, compte du CRM SaaS, outils de communication sensibles) sont protégés par une MFA robuste. Cette mesure complique fortement l'exploitation d'un vol d'identifiants (phishing, fuite de mots de passe), réduisant le risque d'intrusion sur des comptes privilégiés. En cas d'alerte de compromission d'un compte, la MFA agit comme un filet de sécurité limitant

l'accès non autorisé. Pour notre implementation dans ce projet, nous avons forcé google_authenticator comme moyen de double authentification de ssh.

6. **Sauvegardes régulières** – Une politique de sauvegarde est en place pour les données et configurations des systèmes critiques (sauvegardes quotidiennes du cloud et de l'ERP local, images systèmes des drones, etc.), stockées de façon sécurisée y compris hors site. Ces sauvegardes, testées régulièrement, sont essentielles pour pouvoir restaurer les opérations lors de la phase de récupération, notamment après une attaque de type ransomware chiffrant les données.

1. Détection

Objectif : Identifier rapidement tout événement inhabituel pouvant indiquer un incident de sécurité. La détection repose à la fois sur la **surveillance technique** et la **vigilance humaine**.

- **Surveillance automatisée:** Les systèmes de sécurité (EDR => WAZUH, DLP => MyDLP, SIEM & Journalisation => ELK) génèrent des **alertes** en cas d'activité anormale.
    - *Par exemple*, l'EDR peut alerter sur la présence d'un malware ou d'un chiffrement massif de fichiers (symptôme d'un ransomware), le SIEM peut signaler des connexions suspectes sur le VPN ou le CRM SaaS, et le DLP peut notifier un envoi inhabituel de fichiers volumineux vers l'extérieur. Ces alertes sont transmises immédiatement au RSI et aux administrateurs (Wazuh Manager et Dashboard ELK)

- **Signalement par les utilisateurs*:*** En parallèle, chaque collaborateur doit signaler sans délai tout indice d'incident. **Tous les employés connaissent la procédure d'alerte et le contact à joindre en cas d'incident (le RSI)** [Règle 38].
    - *Par exemple*, si un utilisateur reçoit un courriel de phishing ou constate un comportement étrange sur son poste (ralentissements extrêmes, fenêtre de rançon à l'écran, fichiers renommés), il **alerte aussitôt** le RSI (via le canal établi : numéro d'urgence interne ou messagerie dédiée) et se conforme aux consignes immédiates (déconnecter le câble réseau de son PC, etc. si demandé). De même, un ingénieur terrain qui repère une anomalie sur un drone (ex. trajectoire non programmée, envoi de

données inhabituel) le remonte immédiatement.

- **Consolidation des alertes**: À chaque alerte ou signalement, le RSI consigne les informations initiales (qui/quoi/quand/où). Un **ticket d'incident** est ouvert dans le registre prévu, avec une première description de l'événement. Cette traçabilité initiale alimente la suite du traitement. *Si l'alerte provient d'un outil automatique*, les données associées (logs, fichier suspect, capture d'écran) sont collectées. *Si elle provient d'un utilisateur*, le RSI peut poser quelques questions de clarification rapidement (sans retarder l'action) pour comprendre les symptômes.

2. Qualification

Objectif : Analyser l'alerte afin de confirmer qu'il s'agit bien d'un incident de sécurité, en déterminer la nature, l'ampleur et la criticité, pour orienter la réponse. La qualification est une étape cruciale visant à **obtenir la vision la plus fiable possible de la situation** avant d'agir.

Dès qu'une alerte est reçue, le **RSI (avec l'aide des équipes techniques)** mène une enquête rapide : il rassemble les informations disponibles et cherche des **indicateurs de compromission**. Concrètement, cela inclut :

- **Validation de l'incident :** Vérifier qu'il ne s'agit pas d'une fausse alerte ou d'un simple problème technique. Pour cela on consulte les **journaux systèmes et de sécurité** (ex. logs du SIEM, logs des serveurs cloud, traces réseau) et on analyse les alertes de l'EDR WAZUH. On recoupe avec le témoignage utilisateur le cas échéant.
  - *Exemple :* une alerte DLP sur un transfert de fichier peut être corrélée avec l'activité de l'utilisateur à ce moment pour voir s'il s'agit d'un transfert légitime ou d'une possible exfiltration malveillante. *Si un poste semble infecté*, on confirme en identifiant le processus suspect ou le fichier malveillant en quarantaine.

- **Identification du type d'attaque et de l'ampleur :** Une fois l'incident avéré, le RSI caractérise **la nature de la menace** (malware, ransomware, tentative de phishing ayant réussi, intrusion réseau, fuite de données, etc.) et **le périmètre impacté**. Qui ou quoi est touché ? (Un seul poste utilisateur ? Plusieurs ? Un serveur ? Un drone IoT précis ? Des données sensibles ont-elles fuité ?). Il s'agit

d'**étendre l'analyse** pour savoir si d'autres signes existent ailleurs dans le SI : autres machines présentant des symptômes similaires, alertes contemporaines sur d'autres systèmes… On ne doit **pas se limiter à l'équipement signalé initialement**, car une attaque peut être plus large. Ainsi, les administrateurs vérifient par exemple d'autres postes via l'EDR (scan des indicateurs de compromission), examinent le trafic réseau pour repérer d'éventuelles communications avec un serveur de commande pirate, etc.

- **Évaluation de la criticité :** Le RSI évalue **l'impact actuel et potentiel**. Cela comprend : la sensibilité des systèmes ou données affectés (ex. données client dans l'ERP ou bien poste bureautique standard), le niveau de perturbation opérationnelle (arrêt de service, lenteurs, perte de fonctionnalité), et les **risques d'aggravation** si rien n'est fait (propagation du ransomware à d'autres PC, exfiltration continue de données, etc.). On estime également si des obligations réglementaires pourraient s'appliquer (par ex. données personnelles compromises devant être déclarées). Cette évaluation guide l'urgence et l'échelle de la réponse.
    - *Par exemple*, la compromission d'un serveur cloud contenant des données client critiques sera jugée **critique** (priorité absolue, mobilisation de ressources immédiates, communication à la direction) tandis qu'un malware isolé sur un poste isolé pourra être géré en interne sans escalade majeure.

À l'issue de la qualification, le RSI décide **du plan d'action immédiat**. Il informe la Direction si l'incident est grave (pour activation éventuelle d'une cellule de crise interne) et alerte les membres pertinents de l'équipe de réponse (administrateurs, devs, etc.). L'objectif est d'**opposer sans tarder les mesures proportionnées à la gravité de l'incident** – autrement dit, préparer le **confinement** de la menace et la **remédiation**, adaptées au périmètre affecté.

(NB : Si la qualification requiert des compétences pointues non disponibles en interne : par ex. analyse forensic avancée d'un malware inconnu , le RSI peut décider de faire appel à un prestataire extérieur spécialisé en réponse à incident pour appuyer l'équipe.)

3. Réponse initiale et confinement

Objectif : Contenir l'incident le plus rapidement possible afin d'en limiter l'impact et la propagation. Dès que l'incident est **confirmé** et **qualifié**, l'équipe de réponse déploie des mesures d'**endiguement**. Il s'agit d'**isoler la menace** et de **protéger les ressources saines**, tout en évitant de détruire des preuves. Les actions typiques de confinement incluent :

- **Isolation des systèmes compromis : Déconnecter du réseau les machines affectées** pour empêcher toute propagation. Concrètement, un administrateur réseau peut couper le port Ethernet du poste compromis ou le Wi-Fi, le RSI peut ordonner à l'utilisateur de débrancher immédiatement son câble réseau. *Si l'EDR le permet*, il enclenche à distance un *containment* du poste (isolement réseau automatique). *Dans le cas d'un serveur cloud* (CRM dans notre projet), on peut le désactiver temporairement ou au moins bloquer son accès (groupe de sécurité, firewall) en attendant d'en savoir plus. *Pour un drone IoT compromis*, l'ingénieur terrain peut le mettre hors ligne (le faire atterrir et couper sa connectivité). **Des mesures d'urgence comme la coupure segmentée du réseau ou l'arrêt de certains services peuvent être prises** pour stopper l'attaque.
    - *Exemple :* en cas de ransomware en cours de chiffrement, isoler immédiatement le poste infecté et tout partage réseau associé pour protéger le reste du réseau est prioritaire.

- **Blocage des accès et comptes compromis :** *Si l'incident implique une compromission de compte* (par ex. compte utilisateur piraté via phishing), **on suspend ou révoque les accès** de ce compte le temps d'y voir clair. L'administrateur désactive le compte AD ou le compte SaaS concerné, force la déconnexion de toutes ses sessions et impose un changement de mot de passe (une fois l'identité du véritable utilisateur vérifiée pour éviter que l'attaquant ne le change lui-même). De même, *si une clé API ou un jeton d'accès s'est fait voler* (ex. accès cloud), on la révoque immédiatement et on génère de nouvelles clés après coup.

- **Mise en sécurité des sauvegardes et systèmes intacts :** Pour parer à un éventuel effet d'entraînement, **les sauvegardes existantes des données critiques sont immédiatement sécurisées** sur un stockage hors-ligne non affecté. Cela garantit qu'une attaque en cours (ransomware, effacement de données) ne pourra pas détruire les backups. Par ailleurs, *les systèmes non touchés* peuvent faire l'objet de mesures préventives : augmenter la surveillance en temps réel (logs en live), éventuellement déconnecter par précaution des segments non encore compromis si on soupçonne que l'attaquant s'y propage.

- **Préservation des preuves :** Même en urgence, il est crucial de **conserver un maximum d'éléments de preuve** pour l'analyse ultérieure et le diagnostic précis. On **sauvegarde les journaux** pertinents (logs systèmes, logs d'événements de sécurité) en les recopiant sur un support isolé, avant qu'ils ne tournent ou soient effacés.
    - Par exemple, on extrait les journaux du serveur compromis et on les stocke sur un disque externe. Si un malware est identifié, on en garde une copie du binaire suspect pour une éventuelle analyse antivirus approfondie. On note l'heure de chaque action de confinement effectuée.

Il est important de ne pas “nettoyer” trop vite les machines compromises à ce stade, au risque de perdre des indices sur l’attaque ; la suppression définitive viendra dans la phase d’éradication.

- **Communication initiale de crise :** Le RSI informe rapidement les personnes adéquates en interne de la situation, en veillant à contenir la diffusion de l’information pour éviter rumeurs et panique. Par exemple, il peut prévenir le service informatique et la direction : “Incident en cours sur [telle partie du SI], mesures de confinement appliquées, merci de ne pas utiliser [telle ressource] en attendant”. Une communication claire aide à ce que chacun comprenne les restrictions temporaires (ex. “VPN coupé pendant 1h”) et collabore. **Alerte externe :** si l’incident risque de s’étendre à des partenaires ou clients (ex. comptes clients compromis, virus envoyé à l’extérieur), on peut aussi les prévenir rapidement de prendre des mesures de leur côté. *(Les aspects de communication publique et légale sont détaillés dans la section Communication plus bas.)*

En parallèle de ces actions, le RSI évalue s’il est nécessaire de **solliciter de l’aide externe**.

💡 Pour une PME comme AgroRand, il peut s’appuyer sur la plateforme gouvernementale *Cybermalveillance.gouv.fr* pour être mis en relation avec un prestataire d’assistance en cyberincident si besoin. En cas d’incident majeur dépassant les capacités internes (ex. attaque sophistiquée à grande échelle), il peut contacter le CERT-FR de l’ANSSI pour conseil ou signalement. **Notamment, si AgroRand est couvert par une cyber-assurance, l’assureur doit être notifié très tôt** afin de mobiliser l’assistance éventuelle et valider la prise en charge financière.

Toutes ces démarches d’escalade externe doivent idéalement se faire **une fois le périmètre de l’incident circonscrit** par les mesures de confinement ci-dessus (sauf aide d’urgence indispensable en temps réel).

4. Éradication

Objectif : Éliminer la menace des systèmes affectés et combler la faille exploitée, afin que l'incident ne puisse reprendre. Après le confinement, on passe à l'éradication du problème à la source. C'est une étape décisive pour *éradiquer* le malware, l'attaquant ou la vulnérabilité qui a permis l'incident.

Les actions d'éradication vont dépendre de la nature de l'incident :

- **Élimination d'un malware :** Si un virus, ransomware ou autre logiciel malveillant a été détecté, on procède au nettoyage complet des équipements concernés. Souvent, la solution la plus sûre est de **réinstaller à neuf les machines compromises** (reformatage, puis restauration système) pour être certain de supprimer toute présence cachée. *Si ce n'est pas possible immédiatement*, on utilise **l'EDR/antivirus pour supprimer tous les fichiers infectés** et on lance une analyse complète du système. On vérifie également les machines possiblement touchées en secondaire. Par exemple, si un PC a été infecté par un ransomware, on vérifiera que le malware ne s'est pas propagé sur les lecteurs réseau ou envoyé par email à d'autres.

- **Correction de la faille de sécurité :** Si l'incident provient de l'exploitation d'une vulnérabilité (ex. un serveur n'était pas à jour et a été piraté via une faille connue), il est impératif de **corriger cette faille** immédiatement. Cela passe par l'application du **correctif logiciel (patch)** approprié ou, si non disponible, par la mise en place d'une mesure compensatoire (par ex. désactiver le service vulnérable, restreindre son accès). Les administrateurs déploient les mises à jour de sécurité sur *toutes* les machines similaires pour éviter une rechute.
    - *Exemple :* si un exploit a touché un drone via une ancienne version de son firmware, tous les drones IoT du même modèle doivent recevoir la mise à jour firmware corrigée.

- **Suppression des accès persistants de l'attaquant :** Un intrus peut avoir créé des portes dérobées (backdoor) ou laissé des comptes cachés. On effectue donc **un audit des comptes utilisateurs et des accès récents** : suppression ou désactivation de tout compte inconnu ou non autorisé, changement des mots de passe sur les comptes sensibles (comptes admins, comptes de service) par précaution, révocation de toutes les sessions actives.
    - 💡 *De plus, on vérifie les tâches planifiées (tasklist), scripts au démarrage, clés de registre (sur Windows) ou crontabs (sur Linux) pour supprimer tout malware résidant qui tenterait de se relancer.*

- **Nettoyage et vérification finale :** Une fois les actions ci-dessus faites, on réalise une **vérification exhaustive** sur les systèmes affectés : analyses antivirus approfondies, examen des journaux post-incident pour s'assurer qu'aucune activité suspecte ne subsiste, tests de bon fonctionnement. L'objectif est de **garantir que la menace initiale est totalement éliminée** avant de restaurer le service

normal. On profite de cette phase pour durcir la configuration si nécessaire (par ex. renforcer une règle firewall, ajouter une règle de détection au SIEM pour ce type d'attaque).

Durant l'éradication, le **RSI** supervise et valide que toutes les mesures sont bien effectuées. Il peut faire appel aux **développeurs** pour vérifier qu'aucune porte dérobée n'a été ajoutée dans le code des applications internes, et aux **ingénieurs IoT** pour confirmer l'intégrité des drones (par ex. recharger un firmware sain si suspicion de firmware altéré).

(NB : Si un ransomware a chiffré des données, l'éradication consiste à supprimer le ransomware et à sécuriser le système. La question du déchiffrement ou de la restauration des données sera traitée en phase de récupération, Comme on l'entend toujours, il est fortement déconseillé de payer une rançon, et plutôt de s'appuyer sur les sauvegardes, voir ci-après.)

5. Récupération

Objectif : Restaurer et remettre en service les systèmes et données impactés pour un retour à la normale le plus vite possible, en s'assurant que l'incident est résolu. Une fois la menace neutralisée, AgroRand doit **récupérer ses capacités opérationnelles**.

Les étapes de récupération incluent :

- **Restauration des données et systèmes** : Si des fichiers ou bases de données ont été encryptés, détruits ou rendus inaccessibles pendant l'attaque, on procède à leur **restauration depuis les sauvegardes** saines. Grâce à la politique de sauvegarde régulière, AgroRand dispose de copies récentes des données critiques (ex. base ERP, données de drones, configurations serveurs). Les administrateurs restaurent ces données sur des machines propres. S'il a fallu réinstaller des machines ou déployer de nouvelles instances cloud, on y **réimporte les données sauvegardées** pour retrouver l'état opérationnel.
    - *Exemple :* après un ransomware sur un serveur de fichiers, on repart d'une sauvegarde de la veille pour retrouver les fichiers.

- **Remise en service contrôlée :** Avant de rouvrir un système au réseau ou aux utilisateurs, on effectue des **tests** pour vérifier que tout fonctionne normalement et que l'incident ne se reproduit pas. On **confirme que la menace a bien été éliminée** (par des scans antivirus, tests de bon comportement). ***Ce n'est qu'après ces vérifications que le RSI autorise***, en coordination avec les équipes, l***a remise en ligne progressive*** des systèmes affectés.
    - *Par exemple*, on peut d'abord reconnecter un serveur au réseau interne et monitorer son activité de près pendant quelques heures avant de rouvrir l'accès aux utilisateurs externes. On surveille les indicateurs de compromission pour s'assurer qu'aucune activité suspecte ne recommence.

- **Mesures correctives additionnelles :** La récupération est aussi le moment de déployer des **correctifs finaux** et améliorations suite à l'incident. *S'il manquait un patch de sécurité*, **on s'assure que cette fois il est appliqué partout.** On peut aussi renforcer certaines configurations : par ex., après une attaque, imposer une **rotation immédiate de tous les mots de passe** des utilisateurs par précaution (et activer MFA si pas déjà fait pour tous les postes), ou durcir les politiques de sécurité (augmenter la fréquence des sauvegardes, ajouter un filtrage mail anti-phishing plus strict suite à une campagne malveillante, etc.). L'incident sert de déclencheur à ces durcissements pendant que l'attention est maximale.

Une fois les systèmes rétablis, le **RSI valide le retour à la normale** en accord avec les métiers impactés (par ex., le responsable métier confirme que l'ERP fonctionne correctement, le service commercial que le CRM SaaS est à jour, etc.). Il reste cependant vigilant dans les jours qui suivent : l'IT peut maintenir un niveau de **supervision renforcée** sur les éléments restaurés, afin de détecter immédiatement si un comportement anormal réapparaît (signe que l'attaque tenterait de revenir). Cette prudence post-incident assure qu'on ne relâche pas trop tôt les efforts de sécurité.

6. Communication

Objectif : Informer de manière appropriée toutes les parties prenantes de l'incident, en interne comme en externe, conformément aux obligations et à la stratégie d'entreprise. La communication doit être gérée avec précaution pour **garder la confiance** des collaborateurs, clients et partenaires, tout en respectant les obligations légales.

- **Interne (intervenants et direction)** – Tout au long de la gestion de l'incident, le RSI maintient informés les acteurs internes concernés : équipe IT, direction générale, et éventuellement managers des services touchés. Il s'assure d'une **communication régulière** sur l'état de la situation (confiné/en cours de résolution/rétabli), afin que chacun sache quoi faire. *En cas d'impact sur l'organisation du travail* (ex. service indisponible temporairement), les employés sont tenus informés des mesures de contournement ou consignes (par exemple utilisation d'une solution alternative si l'outil principal est hors service). *Une fois l'incident résolu*, **un message interne de clôture peut être diffusé** pour expliquer en termes simples ce qu'il s'est passé et rassurer sur le retour à la normale, tout en rappelant éventuellement les bonnes pratiques (ce dernier point rejoint la sensibilisation).
- **Externe (clients, partenaires, autorités)** – La nécessité de communiquer vers l'extérieur dépend de la nature de l'incident :
    - Si des **clients ou partenaires** sont impactés (par ex. indisponibilité d'un service cloud que propose AgroRand, fuite de données client, retard de livraison causé par l'incident), il convient de les informer de manière transparente et professionnelle. Un communiqué ou des emails dédiés **peuvent être préparés par le RSI** en collaboration avec la direction **et éventuellement l'équipe communication**. On y décrit brièvement l'incident (*sans trop de détails techniques potentiellement anxiogènes*), les mesures prises pour le résoudre et pour éviter que cela ne se reproduise, ainsi que les implications pour le client (ex. « vos données ont pu être exposées, nous vous invitons à changer votre mot de passe » ou « le service X sera de nouveau opérationnel sous 24h »). Cette communication doit être validée par la Direction.

    - En cas d'**incident impliquant des données personnelles**, **une notification à la CNIL sous 72h est obligatoire** (conformément au RGPD). Le RSI, en coordination avec **le délégué à la protection des données** (DPD) s'il existe, devra préparer le dossier de notification indiquant la nature de la violation, le nombre de personnes affectées, les mesures correctives prises, etc. De même, les personnes concernées (clients ou employés dont les données ont fuité) devront possiblement être informées directement si l'incident est susceptible d'engendrer un risque élevé pour leurs droits (ex. vol de données très sensibles, mots de passe compromis...). AgroRand s'engage à respecter strictement ces obligations légales de transparence.

    - Si l'incident revêt un caractère **malveillant (cyber attaque avérée)** constituant une infraction (ex. intrusion, vol de données, rançongiciel), **porter plainte** auprès des autorités (police/gendarmerie) est fortement conseillé. Cela permet de déclencher une enquête officielle et peut apporter une couverture juridique à l'entreprise en cas de dommages. Le RSI préparera les éléments

techniques pour la plainte (rapport d'incident synthétique, preuves conservées) que la Direction pourra déposer.

- Si AgroRand dispose d'une **assurance cybersécurité**, comme mentionné plus haut, **l'assureur doit être informé dès le début**. Outre la prise en charge financière éventuelle, l'assureur peut mandater des experts et conseiller sur la gestion de crise. Le respect des clauses de notification de l'assureur est donc un point de communication à ne pas négliger.

- **Autres autorités ou instances à alerter :** selon le secteur d'activité et les engagements contractuels, AgroRand vérifie s'il faut notifier l'incident à d'autres régulateurs ou partenaires. Par exemple, si un client important l'exige contractuellement, ou si AgroRand participait à un programme de partage d'indicateurs cyber avec une CERT sectorielle. Le RSI, avec le service juridique, s'assure de remplir ces obligations de notification.

En résumé, la communication externe doit être honnête sans être alarmiste, et montrer qu'AgroRand prend la situation en main de façon responsable. Tout message public (communiqué de presse, réseaux sociaux) sera validé par la Direction pour aligner avec la stratégie de l'entreprise et maîtriser l'impact réputationnel.

7. Journalisation

Objectif : Enregistrer de manière détaillée tous les faits, actions et éléments recueillis pendant l'incident. La journalisation constitue la mémoire de l'incident, utile pour l'analyse a posteriori et comme dossier de référence (notamment en cas d'enquête ou de démarche assurance).

Dès le début de l'incident et tout au long du traitement, le RSI ou un membre désigné de l'équipe tient à jour un **journal d'incident** (souvent sous forme d'un document horodaté ou d'un ticket dans un outil ITSM). On y consigne :

- **La chronologie des événements** : heure de la détection (alerte ou signalement initial), heure de chaque action significative (isolement d'un poste, coupure d'un serveur à telle heure, déploiement d'un patch, restauration lancée à telle heure, etc.), heure du rétablissement

final. Cette timeline horodatée permettra de retracer l'incident précisément.

- **Les actions entreprises et décisions** : pour chaque étape, décrire brièvement l'action (ex. "14h07 : EDR a isolé le poste PC-007 de M. Dupont", "14h15 : sauvegarde du serveur ERP effectuée", "14h20 : coupe du réseau segment IoT", "15h10 : mise à jour de sécurité KB12345 appliquée sur serveur cloud"). Noter également les décisions prises en cellule de crise (ex. "décision de notifier la CNIL à 16h").

- **Les éléments de preuve collectés** : liste des fichiers suspects extraits (hash, nom, emplacement), copies d'écran, logs sauvegardés (avec référence du fichier ou du stockage où ils sont conservés), etc. Chaque item est décrit pour qu'on sache ce qui a été récupéré. Par exemple : "Fichier malveillant *ransom.exe* récupéré sur PC-007 (hash SHA-256 …), stocké sur support forensic 01".

- **Les communications effectuées** : noter quand et à qui des communications ont été faites (ex. "15h30 : email informatif interne envoyé à l'équipe X", "16h00 : déclaration CNIL soumise", "16h30 : appel téléphonique à l'assureur").

Ce journal doit être **centralisé et sauvegardé** de façon sécurisée (il peut contenir des informations sensibles). Idéalement, il est stocké dans un espace réservé accessible au seul groupe restreint en charge de l'incident. Il pourra servir de base à la rédaction du rapport d'incident final.

En plus du journal narratif, la journalisation technique consiste à **archiver les journaux systèmes et traces** liés à l'incident. AgroRand veille à conserver ces logs pendant une durée suffisante, soit dans le SIEM, soit par export des portions pertinentes. Cela inclut par ex. les logs d'événements Windows, les journaux du firewall au moment de l'attaque, les en-têtes des emails de phishing reçus, etc. Ces données brutes seront précieuses pour l'analyse approfondie et le retour d'expérience.

8. Retour d'expérience (Post-mortem)

Objectif : Tirer les leçons de l'incident afin d'améliorer en continu la posture de sécurité et la gestion future des incidents. Une fois l'incident clos (systèmes restaurés et opérationnels, urgence passée), AgroRand organise un **débriefing complet** à froid, impliquant tous les acteurs internes ayant participé.

Le RSI animera une **réunion de retour d'expérience (RETEX)** dans les jours qui suivent la résolution. Lors de cette session, on **reprend le fil de l'incident de A à Z** – de sa détection initiale jusqu'à la récupération finale – et on analyse : **qu'est-ce qui a bien fonctionné et qu'est-ce qui est perfectible** dans la réponse apportée. Quelques questions directrices :

- *Détection* – L'incident a-t-il été détecté assez rapidement ? Les outils de supervision ont-ils joué leur rôle correctement (alerte EDR/SIEM) et les utilisateurs ont-ils réagi comme attendu (signalement immédiat) ? Y a-t-il eu des signes précurseurs manqués ?

- *Diagnostic/qualification* – Avons-nous eu toutes les informations nécessaires à temps pour bien qualifier l'incident ? Les procédures d'escalade interne ont-elles été efficaces (alerte de la direction, convocation de l'équipe technique) ?

- *Confinement* – Les mesures d'endiguement prises ont-elles suffi à stopper la menace à temps ? Par exemple, l'isolement réseau a-t-il été fait sans délai ? Aurait-on pu agir plus vite ou de manière plus ciblée pour limiter encore davantage l'impact ? Inversement, y a-t-il eu des conséquences imprévues (arrêt d'un service critique non touché) ?

- *Éradication et récupération* – A-t-on entièrement éradiqué la menace du premier coup, ou y a-t-il eu des résurgences ? Les outils (antivirus, scripts de nettoyage, etc.) et les correctifs ont-ils été adéquats ? La restauration des données a-t-elle été complète et suffisamment rapide pour le métier ? Les plans de reprise d'activité ont-ils bien fonctionné (ou faut-il les adapter)eure.gouv.frcloud-store.fr?

- *Communication* – La communication interne a-t-elle été suffisante (ni trop peu d'informations, ni surabondante) ? Les collaborateurs impactés ont-ils été bien accompagnés (ex. support aux utilisateurs ayant perdu des données) ? La communication externe a-t-elle été gérée de manière appropriée (délai, contenu) ? Devrait-on impliquer d'autres personnes (ex. un porte-parole dédié) la prochaine fois ?

- *Organisation et rôles* – La coordination de l'équipe d'incident a-t-elle été fluide ? Chaque intervenant connaissait-il bien son rôle et ses tâches ? Faut-il prévoir des formations ou ajustements (par ex. former davantage d'administrateurs à l'analyse forensic, ou sensibiliser les utilisateurs suite à un phishing qui a trompé plusieurs d'entre eux) ?

Durant cette réunion, **tous les participants sont encouragés à partager librement** leur point de vue sur ce qui s'est passé. Une atmosphère ouverte et constructive est importante pour obtenir un retour d'expérience honnête. Le RSI documente les conclusions et pistes d'amélioration dégagées.

Les suites typiques d'un RETEX d'incident peuvent inclure : la **mise à jour des procédures** (par exemple, ajuster ce document si une étape manquait ou était mal comprise), le **renforcement de certaines mesures de sécurité** (ex. déployer un nouvel outil si une faille a été identifiée, comme un meilleur filtrage anti-phishing si l'attaque est passée par l'email), des **actions de formation/sensibilisation** supplémentaires (reformer les utilisateurs sur la détection de phishing, exercices de simulation d'incident pour l'équipe IT), ainsi qu'une éventuelle **mise à jour de l'analyse de risques** de l'entreprise pour intégrer le scénario vécu et sa probabilité d'occurrence. Par ailleurs, le RSI s'assure de **capitaliser les enseignements** en les partageant avec les autres équipes de l'entreprise ou confrères du domaine si pertinent, dans une logique d'amélioration globale de la sécurité.

Enfin, le rapport final d'incident, combinant le journal complet et le retour d'expérience, est présenté à la direction d'AgroRand. Il permet à la direction d'apprécier l'incident (impact, gestion, coûts) et de valider les plans d'action résultants. Cela renforce la culture de sécurité de l'entreprise : chaque incident, même fâcheux, devient une **opportunité d'apprentissage** afin de mieux se protéger à l'avenir.

Conclusion

Cette procédure de gestion des incidents de sécurité d'AgroRand, alignée sur les recommandations de l'ANSSI et adaptée à notre contexte spécifique, assure une réponse structurée et efficace face aux cybermenaces identifiées. Elle sera diffusée à l'ensemble du personnel (notamment aux nouveaux arrivants) afin que chacun connaisse son rôle en cas d'incident. Des exercices périodiques (*tests*) pourront être organisés pour entraîner l'équipe technique et valider le bon fonctionnement des outils (EDR, sauvegardes, etc.). **La réactivité, la coordination et l'amélioration continue** sont les maîtres-mots : en appliquant rigoureusement ces procédures, AgroRand se donne les moyens de limiter l'impact des incidents de sécurité et de protéger au mieux ses actifs ainsi que la confiance de ses clients et partenaires.

Sources :

Guide d’hygiène informatique de l’ANSSI (mesures 39 et 40)

Lien 1

Lien 2

Conseils CERT-FR sur la qualification et la réaction aux incidents et Obligations légales (CNIL)

cert.ssi.gouv.fr;

Guide NIST/Cloud Store sur le cycle de réponse aux incidents

cloud-store.frcloud-store.fr.