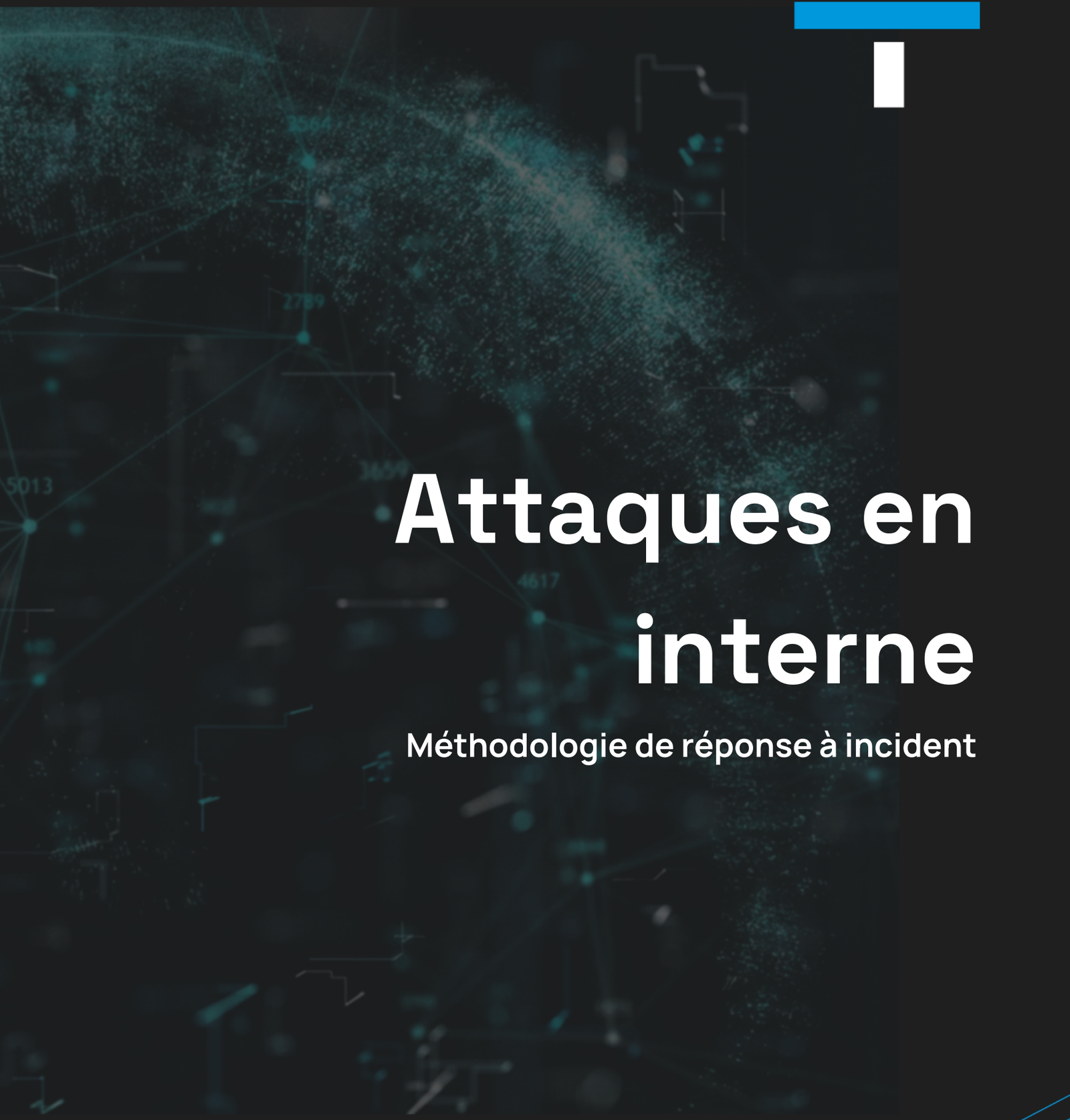
aDvens

Security for the greater good



Attaques en interne

Méthodologie de réponse à incident

IRM-12 | 2022-11-30 | **TLP-CLEAR** | CERT aDvens - CSIRT
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

→ La fiche IRM s'adresse aux personnes ou fonctions suivantes :
- Les **RSSI et leurs adjoints**
- Le **CERT**
- Le **SOC**
- Les **administrateurs**

Dans le cas d'un incident : Lire l'IRM et prendre des notes.
Rester calme et contacter immédiatement l'équipe de réponse à incident du secteur d'activité ou un CERT si nécessaire.

Étapes de traitement des incidents

6 étapes sont définies pour gérer les incidents de sécurité :

1. **Préparation** : Se préparer à gérer l'incident,
2. **Identification** : Détecter l'incident,
3. **Confinement** : Limiter l'impact de l'incident,
4. **Remédiation** : Supprimer la menace,
5. **Récupération** : Revenir à un état normal,
6. **Capitalisation et apprentissage** : Élaborer et améliorer les processus.

Cette IRM fournit des informations détaillées pour chaque étape. Les étapes sont issues du NIST.

Cette fiche est issue du travail collaboratif avec le **CERT-SG** de modification et de mise à jour de leurs fiches de méthodologie de réponse à incident.

Références

→ IRM CERT-SG
→ IRM CERT-aDvens

1. Préparation

Objectif : Établir des contacts, définir des procédures, recueillir des informations et se familiariser avec les outils de détection d'intrusion pour gagner du temps lors d'une attaque.

1.1. Contacts

- S'assurer d'avoir des points de contact dans l'équipe de relations publiques (institutions de régulation), l'équipe de ressources humaines et le service juridique,
- Centraliser la gestion des accès,
- S'assurer d'avoir les autorisations et un processus clair. Ce dernier doit être particulièrement claire sur la suppression des droits d'anciens employés,
- Mettre en place des authentifications fortes en fonction des risques business,
- Préparer la stratégie de communication interne et externe,
- Préparer le processus de prévention de fuite d'information (DLP, Data Loss Prevention) avec les équipes RGPD et de gestion des risques.

Être en mesure d'informer les fournisseurs impliqués, les forces de l'ordre et les régulateurs si nécessaire lors d'un incident (gestion de crise cellulaire).

2. Identification

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

2.1. Identification technique

- → Alertes d'un SIEM ou des outils de corrélation :
  - Un comportement malveillant a pu être détecté grâce à la corrélation de plusieurs événements anormaux.
- → Alertes d'un IDS/IPS détectant une intrusion :
  - Au cas où l'employé tenterait de pirater le système, un système de détection d'intrusion (ou système de prévention d'intrusion) peut être en mesure de déclencher une alerte.
- → Alertes des contrôles et services de DLP :
  - Outils et processus pour détecter et prévenir les violations de données et l'exfiltration de données.
- → Alertes des contrôles d'accès physiques.

2.2. Identification humaine

- → Le management :
  - Le responsable de l'employé pourrait être le premier à remarquer un comportement suspect.
- → Les équipes de contrôle, risque, conformité :
  - Ces équipes disposent de leurs propres systèmes pour détecter les anomalies opérationnelles et peuvent également déclencher des alertes si quelque chose d'anormal est détecté.
- → Les collègues :
  - Les collègues peuvent être le canal de notification le plus précieux car ils connaissent parfaitement les tâches, le processus et les impacts de leur travail. Ils peuvent facilement détecter un comportement suspect.
- → Les parties externes :
  - Les partenaires ou structure externes peuvent également disposer de leurs propres capacités de détection,
  - Si des opérations ont été falsifiées en interne, ces entités externes peuvent apporter une aide précieuse.

Pour plus de détails voir l'IRM-02 ou l'IRM-03, intrusion Windows ou Linux.

3. Confinement

Objectif : Atténuer les effets de l'attaque sur l'environnement ciblé.

Ne rien faire sans une demande écrite du CISO/DPO/responsable concerné.
Sur la base des conseils de l'équipe juridique, une autorisation écrite de l'utilisateur concerné peut également être utile.

1. Impliquer les gens :
   - Les experts doivent être informés de l'incident afin qu'ils puissent apporter leur aide,
   - Cela comprend la gestion des ressources humaines, la gestion juridique, l'équipe DLP, la gestion des relations publiques et la gestion commerciale de l'employé suspect.

2. Réunion :
   - Un responsable RH doit rencontrer l'employé suspect pour lui expliquer ce qui a été découvert et ce qui va se passer,
   - Le soutien de personnes juridiques, techniques et du manager peut être demandé.

3. Réduction des privilèges :
   - Si l'employé suspect est autorisé à rester au travail jusqu'à la fin de l'enquête, lui fournir un ordinateur avec des autorisations minimales.

4. Gel des autorisations :
   - Suspendre les accès et les autorisations de l'employé suspect.
   - Suspendre les accès aux applications. Cela peut également inclure le compte utilisateur, les clés, le badge d'accès du bâtiment.

5. Accès à distance :
   - Suspendre les accès distants, c'est-à-dire : smartphones, comptes VPN, tokens ...

6. Saisie :
   - Saisir tous les appareils informatiques professionnels de l'employé suspect.

3.1. Cas 1 : activité anormale

Si rien de malveillant ou de frauduleux n'est encore confirmé, deux enquêtes devraient commencer dès maintenant :

→ Investigation numérique sur les appareils informatiques de l'employé suspect,
→ Investigation sur les journaux d'audit des différents composants.

Pour plus de détails voir l'IRM-02 ou l'IRM-03, intrusion Windows ou Linux.

3.2. Cas 2 : activité malveillante / frauduleuse

Si un comportement malveillant ou frauduleux est déjà confirmé, penser à porter plainte contre l'employé suspect.

Dans ce cas :

→ Ne pas entreprendre d'autres actions techniques,
→ Fournir à l'équipe juridique ou à l'agent des forces de l'ordre toutes les preuves demandées et être prêt à aider sur demande,
→ Si des dommages collatéraux peuvent résulter de l'abus :
   - S'assurer de contenir les impacts de l'incident avant de le rendre public,
   - Être sûre d'avoir prévenu les autorités si nécessaire,
→ Préparer un plan de communication avec l'équipe de communication (clients, partenaires).

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

La partie remédiation est limitée en cas d'abus d'un employé. Les actions suivantes peuvent être envisagées selon le cas :

- → Prendre des mesures disciplinaires contre l'employé malveillant (ou résiliez le contrat) et supprimer toutes ses identifiants,
- → Passer en revue tous les programmes ou scripts créés par l'employé et supprimer tous les codes inutiles,
- → Examiner les tâches d'administration (équipe informatique).

Informer les fournisseurs impliqués, les forces de l'ordre et les régulateurs, si nécessaire.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Si l'incident n'a pas encore été rendu public :

- → Veiller à avertir toutes les parties prenantes impactées (clients, partenaires concernés…) et les autorités compétentes,
  - Cette communication doit être faite par le top management en cas d'impacts importants.
- → Avertir éventuellement les employés ou les équipes locales du problème pour les sensibiliser et renforcer les contrôles de sécurité.

Revenir en arrière sur les opérations frauduleuses commises par l'employé (restauration d'une sauvegarde par exemple).

6. Capitalisation et apprentissage

Objectif : Documenter les détails de l'incident, discuter des leçons apprises et ajuster/améliorer les dispositifs et stratégies de défense.

Le rapport d'incident

Il doit être rédigé et mis à la disposition de toutes les parties prenantes.

Le retour d'expérience

Les thèmes du retour d'expérience doivent être décrits avec les éléments suivants :

- → Cause initiale de l'infection,
- → Actions et chronologies de chaque événement important,
- → Ce qui s'est bien passé,
- → Ce qui ne s'est pas bien passé,
- → Coût de l'incident,
- → Indicateurs de compromission.

La capitalisation

Des actions d'amélioration des processus de détection des logiciels malveillants et des intrusions sur le réseau doivent être définies pour capitaliser sur cette expérience.