RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en cybersécurité

LES ESSENTIELS

d'un rapport de remédiation post incident

A la suite d'un incident de cybersécurité, le **rapport de remédiation** constitue un livrable central de la prestation. Il permet de documenter les actions entreprises pour contenir, éradiquer et corriger les effets de l'incident, tout en assurant au client une vision claire des causes, des impacts et des mesures préventives mises en œuvre pour éviter toute récurrence.

Le présent document a pour objectif de définir les attendus minimaux essentiels à tout **rapport de remédiation** à remettre au client à l'issue de l'intervention, afin de garantir une traçabilité complète des actions réalisées, une compréhension partagée de la situation et des mesures correctives et une capitalisation sur l'expérience pour renforcer durablement la posture de sécurité de l'organisation.

Les éléments listés ci-dessous seront notamment attendus dans le cadre d'une labellisation ExpertCyber.

01 INTRODUCTION

- **Domaine d'activité** du client et éventuelles réglementations applicables,
- **Contexte** de l'incident,
- **Périmètre** impacté,
- **Services** impactés,
- **Objectifs de l'intervention** (restauration rapide, reprise du contrôle ou préparation à une maîtrise durable du SI…)

02 SYNTHÈSE MANAGÉRIALE

Doit être compréhensible par des personnes non expertes en sécurité des systèmes d'information.

- **Contexte global de l'incident** (acteurs, impacts, portée),
- **Résumé de la compréhension de l'incident** (date, chronologie, cheminement de l'attaquant, fuites éventuelles),
- **Mesures correctives** mises en œuvre,
- **Difficultés rencontrées,**
- **Liste des risques résiduels** (avec niveaux) et **recommandations** les plus importantes.

03 DIAGNOSTIC DE L'INCIDENT

- **Persistance de la menace** (présence de l'attaquant),
- **Objectifs supposés de l'attaquant** (destruction, usurpation, crapuleux...),
- **Date initiale,**
- **Patient Zéro** (vecteur initial),
- **Niveau privilège obtenu,**
- **Latéralisation,**
- **Liste des compromissions.**

04 ANALYSE

- **Indicateurs de compromissions** (recherchés et trouvés),
- **Éléments collectés** (méthodes de collecte),
- **Chronologie des actions** réalisées par l'attaquant,
- **Chemins de compromission.**

05 PLAN D'ACTION DE REMÉDIATIONS (CHRONOLOGIE PRIORISATION)

- **Endiguement de la menace** (mesures d'isolement),
- **Éviction,**
- **Éradication,**
- **Reconstruction.**

06 PROPOSITION D'ACTIONS DE SÉCURISATION COMPLÉMENTAIRES