CHARTE DE BONNE CONDUITE DES ACTEURS DE LA NOTATION CYBER

- La typologie des actifs traités (adresses IP, noms de domaines…) par chaque agence de notation doit être décrite et accessible aux utilisateurs de la notation et aux organisations notées.
- Le référentiel de notation (points de contrôle…) doit être accessible aux utilisateurs de la notation et aux organisations notées.
- L'interaction entre l'acteur de la notation et l'organisation notée ne doit pas être conditionnée à une relation commerciale.
- L'organisation doit pouvoir :
    1. accéder à la cartographie des actifs inclus dans la notation avec les explications associées aux défaillances ;
    2. demander la modification de la cartographie / du périmètre, si nécessaire, avec une correction effectuée dans un délai objectif de 10 jours.
- Un acteur qui émet une notation sur une organisation doit préciser si le périmètre pris en compte est reconnu comme représentatif par l'organisation notée et à quelle date (ce qui augmente l'indice de confiance).
- La logique de l'algorithme de notation et la pondération doivent être identiques, quelles que soient les organisations notées.
- Le système d'information mise en oeuvre par l'agence de notation doit faire l'objet d'une certification en cybersécurité par un tiers.
- La référence de l'algorithme de notation utilisé pour établir une note doit accompagner la note émise.
- Tout changement majeur du système de notation (modification de l'algorithme, référentiel de notation…) devrait être communiqué et accessible a minima aux clients et aux organisations surveillées 3 mois à l'avance (un préavis plus faible pouvant être justifié par la prise en compte d'une menace nouvelle), avec si possible une phase de superposition des notations initiales et nouvelles pendant une période de 6 mois.
- Les agences de notation s'engagent à répondre de manière appropriée aux sollicitations techniques des organisations scrutées, en particulier pour les levées de doute (adresses IP utilisées).

CLUSIF