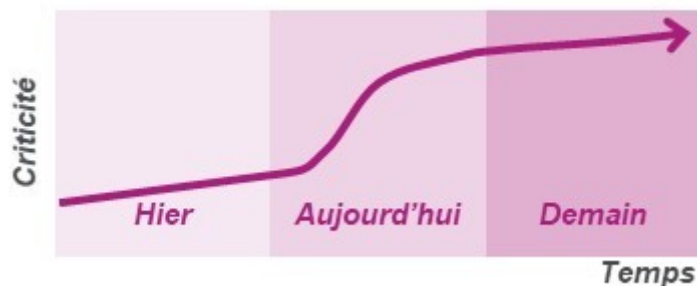


La force et l'horizon d'impact de cette activité critique sont :



- Il s'agit d'une criticité actuelle croissante et qui va se maintenir à l'avenir (court terme / moyen terme / long terme)
- L'enjeu est de toucher 100% des établissements tout au long de la chaîne de valeur

Les leviers de cette activité critique sont :

- Une capitalisation des bonnes pratiques en matière de sensibilisation / formation à la cybersécurité mises en place par les syndicats et les fédérations ; encouragement des approches innovantes à impact (exemple : grille d'évaluation aux risques inspirée du référentiel ANSSI dialoguée avec les donneurs d'ordre de la filière pour disposer d'un référentiel commun partagé et partageable avec l'ensemble de la filière)
- Une mutualisation de ressources à l'échelle de la branche ou du territoire (expert conseil au lancement de la démarche, appui à l'ingénierie financière de prise en charge, AMO / PMO, liste de prestataires recommandés à tarif encadré, offre de service des fédérations, plateforme d'échanges...)

- Des formations aux enjeux de la 5G (technologies associées, business case, nouveaux risques cyber)
- Une communication forte à l'ensemble des collaborateurs et des entreprises sur l'importance d'une bonne maîtrise des enjeux de cybersécurité (sur site et à distance, process, produits et services) ; Des actions et chartes confidentialité / RGPD ; Une sensibilisation de tout le tissu industriel (cycles de rencontres d'entreprises, webinars...)
- Pour les ETI et GE : Une action sur les leviers d'attractivité, notamment au recrutement, face à la concurrence et une valorisation du sens et de la contribution opérationnelle des experts cybersécurité vis-à-vis de la production ou de l'activité de l'entreprise

Référence(s) :

- Activités critiques
Date de publication : 05/2021