

Analyse des risques cyber pour les installations industrielles

Afin de mieux identifier et vous prémunir de risques cyber pouvant impacter vos installations, l'Ineris met en œuvre une méthode d'analyse des risques cyber éprouvée et prenant en compte les spécificités du milieu industriel, en lien avec les études de dangers pour les personnes et l'environnement.

L'Ineris vous propose une démarche en 5 étapes :

Définition du niveau de menace pesant sur vos systèmes

- **Évaluation du contexte** : Analyse des menaces spécifiques à votre secteur d'activité et à vos installations
- **Profil des attaquants potentiels** : Identification des acteurs malveillants susceptibles de cibler vos systèmes, qu'ils soient internes ou externes
- **Prise en compte des tendances** : Intégration des évolutions récentes en matière de cyberattaques dans le milieu industriel

Identification des scénarios de risques et des chemins d'attaques potentiels

- Identification des **systèmes critiques** pour la sécurité des biens, des personnes et de l'environnement
- Modélisation des **scénarios d'attaque** visant ces systèmes
- Évaluation des conséquences potentielles sur la **sécurité des personnes, l'environnement et la continuité des opérations**

Identification du niveau de protection face aux principales vulnérabilités existantes

- Évaluation des **mesures de sécurité** actuelles : Analyse des mesures techniques et organisationnelles en place contre les **vulnérabilités** connues
- Comparaison avec les **bonnes pratiques** : Vérification de l'adéquation de vos mesures de sécurité par rapport aux **standards industriels**

Évaluation des risques associés aux scénarios identifiés

- Analyse de la **vraisemblance** : Estimation de la vraisemblance des scénarios en fonction des vulnérabilités et des menaces identifiées
- Estimation de la **gravité** : Quantification des impacts potentiels sur les personnes, l'environnement et les opérations
- Priorisation des risques : Classement des risques et **hiérarchisation des systèmes et équipements** en fonction de leur criticité pour orienter les actions à mener

Proposition de plans d'action pour maîtriser les risques cyber

- Identification des points faibles : Repérage des domaines où le **niveau de protection** peut être amélioré
- Élaboration de recommandations : Suggestion de **solutions techniques et organisationnelles** pour atténuer les risques identifiés
- Élaboration de recommandations : Suggestion de **solutions techniques et organisationnelles** pour atténuer les risques identifiés