

## **The Common Criteria (CC) « Le critère commun pour évaluer la sécurité IT »**

Le CC est un guide pour le développement et l'évaluation de produits et systèmes de sécurité IT qui a pour but de fournir une assurance de sécurité. Le CC est supporté par le standard international ISO. Une certification CC fournit une garantie d'assurance en mesurant le niveau de sécurité en fonction de la probabilité des menaces et leur impact. Il y a 7 niveaux d'assurance, le premier niveau étant quand la menace et l'impact sont très faibles et le septième étant quand la menace et l'impact sont très forts.

Le document CC est divisé en trois parties :

1. Définition des concepts et principes de l'évaluation de la sécurité IT et présente un modèle général d'évaluation qui a pour but de fixer les objectifs et les exigences IT.
2. Définition des exigences fonctionnelles de la sécurité IT en composant standard de sécurité.
3. Définition des exigences d'assurance de la sécurité IT en cataloguant les composants et en évaluant leur niveau d'assurance.

Le profil de protection répond à la question « What do I need in a security solution » qui définit concrètement ce que veut le client.

La cible de sécurité répond à la question « What do you provide in a security solution » qui sont les bases de l'évaluation.

La méthodologie d'évaluation commune est utilisée lors d'une certification CC afin de décrire les actions et les activités à effectuer par l'évaluateur pour conduire l'évaluation du CC.