# Documentation Préparation à la Certification


Clairon Anthony

Pourquoi ?

Après cette année de BTS SIO en option SISR, je souhaite poursuivre sur une License professionnelle en SRSI ou un Bachelor en administration réseau et système et ensuite possiblement valider un Master en cybersécurité. Il est donc nécessaire que je me sensibilise aux enjeux de la cybersécurité, en particulier dans un contexte professionnel et également maîtriser les techniques de piratage éthique afin d'identifier les failles et de les corriger.

## Choix des certifications :

1- MOOC de l'ANSSI
2- Certification Ethical Hacker

## Certification 1 : MOOC de l’ANSSI

Le MOOC SecNumacadémie est une formation en ligne gratuite proposée par l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Son objectif est de sensibiliser un large public aux enjeux de la cybersécurité, en particulier dans un contexte professionnel.

Le MOOC est structuré en quatre modules, chacun composé de plusieurs unités. Chaque unité aborde des thématiques clés de la sécurité des systèmes d'information, telles que la protection des données, la gestion des mots de passe, ou encore la prévention des attaques informatiques. Les contenus sont élaborés par des experts de l'ANSSI et sont régulièrement mis à jour pour refléter l'actualité réglementaire et technique. secnumacademie.gouv.fr

Pour valider le MOOC et obtenir une attestation de suivi, il m'a fallu :

- Visualiser 100 % des contenus de chaque unité.
- Réussir les quiz finaux avec un score d'au moins 80 % (soit 8 bonnes réponses sur 10).
- Valider l'ensemble des modules.
- Me renseigner et prendre des cours

L'attestation obtenue elle est valorisée professionnel pour démontrer une sensibilisation aux bonnes pratiques en cybersécurité. C’est un bon premier pas vers des certifications professionnels plus poussé.

## Certification CEH avec l’entreprise :

La certification **Certified Ethical Hacker (CEH)** est une accréditation internationale délivrée par l'EC-Council, destinée aux professionnels de la cybersécurité souhaitant maîtriser les techniques de piratage éthique afin d'identifier et de corriger les vulnérabilités des systèmes informatiques.

Le programme CEH forme les participants à penser et agir comme un hacker malveillant, mais dans un cadre légal et éthique. L'objectif est de comprendre les méthodes utilisées par les cybercriminels pour mieux sécuriser les systèmes d'information.

La version 13 du CEH comprend :

- **20 modules** couvrant plus de **550 techniques d'attaque**
- **221 laboratoires pratiques** pour une application concrète des connaissances
- Des compétences en **intelligence artificielle** appliquées à la cybersécurité

Cette formation est reconnue par des institutions telles que le **Department of Defense (DoD)** des États-Unis.

Pour passer l'examen CEH, deux options s'offrent à nous :

1. **Suivre une formation officielle** dispensée par un centre agréé par l'EC-Council.
2. **Justifier de deux ans d'expérience professionnelle** en sécurité de l'information et soumettre une demande accompagnée de frais d'inscription de 100 USD. CERT

Puis passer l’examen:

- **Format** : 125 questions à choix multiples
- **Durée** : 4 heures
- **Note de passage** : Varie entre 60 % et 85 %, selon la version de l'examen.

Après avoir obtenu la certification CEH, il est possible de viser le titre de **CEH (Master)** en réussissant un examen pratique de 6 heures dans un environnement réseau simulé. Cette épreuve évalue la capacité à appliquer les compétences acquises dans des situations réelles.

La certification CEH est valable **3 ans**. Pour la renouveler, il est nécessaire de cumuler **120 crédits de formation continue** pendant cette période.

Dans le cadre de ma formation des ressources et des modules sont déjà à la disposition des personnes il ne tient donc qu’a nous employé de les utiliser. Je compte passer l’examen à la fin de mon cursus de Master ou License pour justifier de mes deux ans d’expérience.