

Khennous Moad
1SIO-B

Compte rendu du MOOC ANSSI – BTS SIO 1ère année

Introduction

Dans le cadre de ma première année de BTS SIO, j'ai suivi et validé le MOOC de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information).

Ce parcours m'a permis d'acquérir une vision globale et progressive de la cybersécurité, organisée en 4 modules et 20 unités.

Ce compte rendu présente ce que j'ai appris, compris et retenu, ainsi que les apports personnels de cette formation essentielle pour le domaine informatique.

MODULE 1 – Panorama de la SSI

Ce premier module m'a permis d'avoir une vue d'ensemble de la cybersécurité, de ses enjeux et de ses acteurs.

Ce que j'ai appris

- La société est devenue un monde numérique hyper-connecté, où chaque appareil et chaque donnée peut être une porte d'entrée pour des attaques.
- Les cybermenaces sont nombreuses : malware, phishing, ransomware, ingénierie sociale, attaques sur les infrastructures, etc.
- Les motivations des attaquants sont variées : vol d'argent, espionnage, sabotage, défi technique, ou cybercriminalité organisée.
- Le cyberspace exige une protection continue car chaque individu et chaque organisation est une cible potentielle.
- La cybersécurité est un écosystème composé de nombreux acteurs : États, entreprises, CERT, ANSSI, utilisateurs, experts SSI.
- Les règles d'or de la sécurité (mises à jour, mots de passe, sauvegardes, prudence en ligne...) sont les bases mais restent trop souvent négligées.

Ce que j'ai compris

- La cybersécurité n'est pas qu'un domaine technique : c'est un enjeu stratégique, économique et humain.
- Chaque utilisateur est un maillon essentiel : un comportement négligent peut compromettre tout un système.
- La sécurité vise à garantir la CIA : Confidentialité, Intégrité, Disponibilité.

Ce que je retiens

- La cybersécurité commence par les bonnes pratiques individuelles.
- Les menaces évoluent constamment : il faut être vigilant et continuellement formé.

Apports personnels

Ce module a renforcé ma compréhension globale des enjeux du numérique. Il m'a permis de mesurer la responsabilité que j'aurai en tant que futur professionnel IT.

MODULE 2 – Sécurité de l'authentification

Ce module m'a aidé à comprendre les mécanismes permettant d'identifier et d'authentifier un utilisateur de manière fiable.

Ce que j'ai appris

- Les 3 grandes catégories d'authentification :
Ce que je sais (mot de passe),
Ce que je possède (clé USB, smartphone),
Ce que je suis (biométrie).
- Les méthodes fortes : double authentification (2FA), OTP, certificats.
- Les attaques courantes sur les mots de passe : brute force, dictionnaire, phishing, keyloggers, fuite de bases de données.
- Les critères d'un mot de passe robuste.
- Les bonnes pratiques de gestion des mots de passe : gestionnaires, renouvellement, segmentation des comptes.

Ce que j'ai compris

- Le mot de passe reste une faiblesse humaine plus qu'une faiblesse technique.
- Beaucoup de compromissions proviennent de mots de passe trop simples ou réutilisés.
- La sécurité repose désormais sur une approche multi-facteurs plutôt que sur un seul secret.

Ce que je retiens

- Utiliser un gestionnaire de mots de passe est indispensable.
- L'authentification doit combiner plusieurs facteurs pour être réellement efficace.

Apports personnels

Ce module m'a poussé à revoir ma propre gestion de mots de passe. J'ai adopté un gestionnaire et activé la 2FA sur la plupart de mes comptes. Cela renforce ma posture professionnelle et personnelle.

MODULE 3 – Sécurité sur Internet

Ce module m'a permis de comprendre les risques liés à l'utilisation quotidienne d'Internet et comment s'en protéger efficacement.

Ce que j'ai appris

- Les bases du fonctionnement d'Internet : client, serveur, protocole HTTP/HTTPS.
- Les risques liés au téléchargement de fichiers : malware, faux sites, logiciels piégés.
- Les dangers liés à la navigation web : trackers, phishing, sites frauduleux, cookies malveillants.
- Sécurisation des messageries : pièces jointes, liens suspects, usurpation d'identité, spam.
- Le fonctionnement réel d'une connexion web (DNS, requêtes, certificats SSL/TLS).

Ce que j'ai compris

- Internet est un environnement ouvert, donc par nature vulnérable.
- La majorité des attaques réussies reposent sur la méconnaissance ou la précipitation de l'utilisateur.
- Le HTTPS ne garantit pas que le site est honnête : il chiffre seulement la communication.

Ce que je retiens

- Toujours vérifier l'URL, la source des pièces jointes et l'émetteur réel d'un message.
- Ne jamais télécharger depuis des sites non officiels.
- Utiliser des outils de filtrage, antivirus et navigateurs à jour.

Apports personnels

J'ai amélioré ma vigilance en ligne. Je me sens plus conscient des signaux d'alerte (URL suspecte, pièce jointe douteuse, faux emails). Cela m'aide autant dans mes usages personnels que dans ma formation informatique.

MODULE 4 – Sécurité du poste de travail et nomadisme

Ce module traite de la sécurisation des appareils et des risques liés à la mobilité.

Ce que j'ai appris

- Importance des mises à jour (système, applications, drivers).
- Configuration de base d'un poste : antivirus, pare-feu, verrouillage automatique, comptes utilisateurs.
- Paramètres de sécurité avancés : chiffrement, sandboxing, gestion des droits.
- Risques liés aux périphériques amovibles : clés USB infectées, vol de données.
- Séparation des usages : personnel / professionnel.

Ce que j'ai compris

- Le poste de travail est la première cible des cyberattaquants.
- Les vulnérabilités viennent souvent des logiciels non mis à jour.
- Le nomadisme (wifi publics, mobilité) augmente les risques d'interception et de vol.

Ce que je retiens

- Toujours verrouiller son poste.
- Ne jamais connecter un périphérique non fiable.
- Utiliser un VPN sur les réseaux publics.
- Respecter la séparation travail/vie personnelle.

Apports personnels

Ce module m'a permis de comprendre l'importance de configurer correctement mes appareils, surtout dans les contextes scolaires et professionnels. Je fais désormais beaucoup plus attention à la gestion de mes périphériques, de mes réseaux et de mes mises à jour.

Conclusion générale

Le MOOC de l'ANSSI m'a offert une vision complète et progressive de la cybersécurité. J'ai acquis des connaissances théoriques solides, mais aussi des réflexes pratiques essentiels pour ma future carrière en informatique.

Ce que je retiens globalement :

- La cybersécurité repose autant sur la technique que sur le comportement humain.
- Chaque utilisateur est un acteur clé de la sécurité.
- Les bonnes pratiques quotidiennes sont souvent les plus simples mais aussi les plus négligées.

Ce MOOC renforce mon intérêt pour la cybersécurité et me conforte dans mon projet de poursuivre dans ce domaine, notamment via ma réorientation future en BTS Cybersécurité.