DECOUVERTE
DE LA CYBERSÉCURITÉ

Presenter par
MOCQUILLON
Lucas

Table des matières

Découverte de la Cybersécurité

Contexte de la formation

Dans le cadre de ma formation, j'ai suivi plusieurs formations en ligne (MOOC) et étudié des guides officiels de la CNIL et de l'ANSSI.

Ces ressources m'ont permis de comprendre les principales menaces qui pèsent sur les systèmes d'information (malwares, ransomwares, attaques par déni de service distribué – DDoS, phishing, etc.), ainsi que les techniques d'attaque les plus courantes et leurs impacts possibles sur la **disponibilité**, l'**intégrité** et la **confidentialité** des données.

Compétences développées

Notions fondamentales de la SSI

J'ai consolidé les notions théoriques et pratiques attendues au niveau BTS SIO :

- **Le modèle D.I.C.T.** (Disponibilité, Intégrité, Confidentialité, Traçabilité) appliqué aux données et aux services, avec mise en pratique sur des exemples concrets (protection de numéros de téléphone, partage de documents, sécurisation des services réseau)
- **Types de menaces et d'attaques** : malwares, ransomwares, phishing, DDoS, compromission de compte, fuites de données, injection SQL, usurpation d'identité
- **Défense en profondeur** : superposition de mesures organisationnelles (sensibilisation, politiques), techniques (pare-feu, segmentation, filtres ACL, antivirus, mises à jour) et physiques
- **Surface d'attaque** : identification et réduction des vecteurs d'attaque par désactivation des services inutiles, filtrage des ports, séparation des environnements

Réseau, segmentation et résilience

Sur le plan infrastructure et réseau :

- **Segmentation réseau** (VLAN, sous-réseaux, vSwitch, VPN) pour isoler les services critiques et limiter la propagation des attaques
- **Gestion des SPOF** (Single Point Of Failure) et introduction à la **haute disponibilité (HA)** : identification des points de défaillance, redondance des équipements clés (routeurs, switchs, liens Internet)
- **Modèle réseau à 3 tiers (3-Tier)** : séparation logique des couches accès, distribution et cœur

- **Listes de contrôle d'accès (ACL)** pour filtrer le trafic entre VLAN et contrôler les accès inter-services
- **Plans de Continuité d'Activité (PCA) et Plans de Reprise d'Activité (PRA)** pour assurer la disponibilité des services critiques
- **Sauvegarde et résilience** : règle 3-2-1 (3 copies, 2 supports différents, 1 hors site), différence entre sauvegarde complète/différentielle/incrémentale, importance des tests de restauration

Authentification et contrôle d'accès

- **Mots de passe robustes** : longueur minimale, complexité (majuscules, minuscules, chiffres, caractères spéciaux), unicité par service
- **Authentification multi-facteurs (2FA/MFA)** lorsque possible, pour renforcer la sécurité des accès sensibles
- Distinction entre **authentification**, **autorisation** et **traçabilité** des actions utilisateurs
- **Principe du moindre privilège** : attribution des droits d'accès minimums nécessaires à l'exécution des tâches (comptes utilisateurs vs. admins, droits sur partages, accès aux applications)
- Risques liés aux **comptes partagés**, mots de passe réutilisés et absence de journalisation

Menaces et vecteurs d'attaque

- Identification des principaux types de malwares, ransomwares, attaques DDoS et phishing
- Compréhension des modes opératoires et des impacts sur les systèmes
- Analyse des vulnérabilités et des risques associés
- Chaîne de l'infection et progression latérale dans les réseaux

Bonnes pratiques de sécurité

Les guides de l'ANSSI (« Appliquer les dix règles d'or préventives ») et les supports de sensibilisation m'ont aidé à formaliser des mesures concrètes de durcissement :

- Gestion des mots de passe (complexité, unicité, authentification multi-facteurs)
- Mises à jour régulières des outils numériques et des systèmes d'exploitation
- Segmentation réseau et contrôle d'accès basé sur le besoin
- Plans de sauvegarde et de continuité d'activité
- Sécurisation des postes de travail (verrouillage, gestion des privilèges, absence de surveillance)
- Protection de la messagerie électronique contre le phishing
- Comportements à adopter face aux e-mails suspects et aux pièces jointes douteuses
- Sensibilisation aux réseaux Wi-Fi publics et aux risques d'interception de données
- Gestion des équipements mobiles et nomadisme sécurisé

Hygiène numérique et sensibilisation utilisateurs

Grâce aux MOOC SecNumAcadémie, SensCyber et aux supports CNIL/ANSSI, j'ai développé une capacité à :

- **Expliquer les risques** cyber de façon accessible à des utilisateurs non techniques (phishing, liens piégés, pièces jointes malveillantes, réseaux Wi-Fi publics, réseaux sociaux)
- Rappeler les **bons réflexes au quotidien** : verrouillage de session, prudence sur les pièces jointes, vérification des URL, mise à jour des équipements, sauvegardes
- Contribuer à la rédaction ou à l'amélioration d'une **charte informatique** (postes de travail, messagerie, Internet, équipements nomades, télétravail)
- Participer à des **actions de sensibilisation** (présentations, supports pédagogiques, mini-scénarios d'attaque/défense)
- Identifier et signaler les comportements à risque au sein d'une organisation

Cadre réglementaire et protection des données

En parallèle, j'ai approfondi le volet conformité et protection des données personnelles à travers plusieurs documents de la CNIL :

- **Guides RGPD** : mise en conformité en 6 étapes, principes de la protection des données, droits des personnes
- **Modèles et bases de connaissances PIA** : Analyses d'Impact relatives à la Protection des Données (AIPD/DPIA)
- **Guide DPO** : rôle du Délégué à la Protection des Données, responsabilités organisationnelles
- **Guide de sécurité personnelle** : protection des données, gestion des risques, mesures techniques et organisationnelles

Compétences acquises au niveau opérationnel :

- Compréhension des **principes du RGPD** (licéité, loyauté, transparence, minimisation des données, limitation des durées de conservation, sécurité, droits des personnes)
- Capacité à **lire et utiliser un registre des traitements** simplifié (finalités, catégories de données, destinataires, durées de conservation, transferts hors UE)
- Familiarisation avec la démarche de **PIA (Analyse d'Impact relative à la Protection des Données)** : identification des risques pour les droits et libertés, prise en compte des mesures de sécurité techniques et organisationnelles
- Connaissance du **rôle du DPO** dans une organisation et de ses interactions avec les équipes techniques et métiers
- Notion de **responsabilité du responsable de traitement** et obligation de démonstration de conformité

Cette partie m'a permis de relier la cybersécurité aux exigences légales : principe de minimisation, registre des traitements, gestion des risques, droits des personnes, analyse d'impact, et gouvernance des données personnelles.

Gestion des risques SSI (approche EBIOS)

Avec le module ANSSI x Club EBIOS, j'ai été initié à la **gestion des risques SSI** de manière structurée :

- Compréhension de la démarche globale : **contexte, événements redoutés, sources de menace, scénarios de menace, mesures de sécurité**
- Capacité à identifier des **actifs essentiels** (données, services, infrastructures) et les impacts potentiels (disponibilité, intégrité, confidentialité, image, conformité)
- Mise en relation entre **scénarios de menace** et **mesures de protection** (techniques, organisationnelles, contractuelles)
- Vision globale de la cybersécurité comme **gestion de risques** et non uniquement comme un ensemble de solutions techniques
- Évaluation de la gravité et de la vraisemblance pour prioriser les actions

Investigation OSINT et recherche d'informations

Le certificat OSINT-FR m'a apporté une première expérience de la **recherche d'information en sources ouvertes** :

- Définition de l'OSINT et ses limites en tant que pratique de cybersécurité
- **Bonnes pratiques de collecte et de croisement d'informations** publiques (moteurs de recherche, réseaux sociaux, registres publics, archives, etc.)
- **Respect du cadre légal et éthique** dans l'utilisation des données collectées
- Intérêt de l'OSINT pour la cybersécurité : recherche d'indices de compromission publics, veille de sécurité, intelligence sur les menaces

---

Ressources de formation consultées

Formation	Organisme	Thématique	Date	Résultat
Atelier RGPD - Module 1 à 6	CNIL	RGPD, principes, responsabilités, DPO, collectivités, travail	18-20 août 2025	100% (modules 1-5), 83% (module 6)
SecNumAcadémie - 4 modules	ANSSI	Panorama SSI, authentification, Internet, poste de travail nomadisme	13 août 2025	100% (tous modules)
SensCyber	Platform SensCyber	E-sensibilisation, bonnes pratiques, protection collective	25 avril 2025	Attestation
MOOC OSINT-FR	OSINT-FR	Investigation en sources ouvertes, concepts fondamentaux, outils	19 novembre 2025	Complété
Test ANSSI x Club EBIOS	ANSSI / Club EBIOS	Méthode EBIOS, analyse de risques SSI	21 octobre 2025	100% (6/6)
Présentation SIO2 - Rappel cybersécurité	Campus St Félix-La Salle	Vulgarisation menaces, modèle DICT, architecture réseau, SPOF	Continu	Référence pédagogique

---

Documents de référence étudiés

Guides CNIL

- **Guide RGPD - Se préparer en 6 étapes** : Démarche de conformité avec étapes clés (désigner un pilote, cartographier les traitements, prioriser, gérer les risques, organiser les processus, documenter)
- **Guide RGPD - Sécurité personnelle** : 18 fiches thématiques couvrant sensibilisation, authentification, gestion des accès, traçabilité, sécurité des postes, informatique mobile, réseau, serveurs, sites web, sauvegardes, archivage, maintenance, sous-traitance, échanges, locaux, développements, chiffrement
- **PIA - Modèles (PIA-2)** : Outils et modèles pour conduire une Analyse d'Impact relative à la Protection des Données
- **PIA - Bases de connaissances (PIA-3)** : Catalogue complet de mesures de sécurité, typologies de risques, évaluations de gravité et vraisemblance, menaces d'accès illégitime, modification, disparition de données
- **Guide Délégué à la Protection des Données (DPO)** : Rôle du DPO, désignation, missions, moyens, statut, accompagnement, annexes pratiques (lettre de mission, formulaire de désignation)

Guides ANSSI

- **Appliquer les dix règles d'or préventives** : 10 bonnes pratiques élémentaires de cybersécurité (séparation usages personnel/professionnel, mises à jour, authentification forte, surveillance des équipements, protection des informations personnelles, sécurité messagerie, Wi-Fi public, sauvegardes, antivirus, privilèges)

Supports de cours

- **Présentation SIO2 - Rappel cybersécurité (v1)** : Vulgarisation des menaces, cadre DICT (Disponibilité, Intégrité, Confidentialité, Traçabilité), modèle SMSI, architecture réseau et redondance, prévention des SPOF, gestion des risques, conception de réseaux à 3 tiers, plan d'action en cas d'incident

---

Résumé de la formation

L'ensemble de ces contenus constitue un socle solide et progressif de découverte de la cybersécurité, abordant **quatre dimensions complémentaires et inséparables** :

1. Dimension technique et infrastructurelle

Comprendre les menaces (malwares, ransomwares, DDoS, phishing) et mettre en œuvre des mesures de protection concrètes : gestion des mots de passe, mises à jour, segmentation réseau, sauvegardes, durcissement des postes, redondance des services critiques et réduction des SPOF.

2. Dimension organisationnelle et gouvernance

Sensibiliser les utilisateurs, établir des politiques de sécurité cohérentes, mettre en place une gouvernance des données (rôle du DPO, SMSI, gestion des risques), assurer la traçabilité des actions et maintenir une culture de sécurité.

3. Dimension réglementaire et légale

Assurer la conformité RGPD, protéger les données personnelles, analyser les impacts sur la vie privée, respecter les droits des personnes, documenter la conformité et démontrer la mise en œuvre de mesures appropriées.

4. Dimension opérationnelle et proactive

Rechercher et collecter des informations sur les menaces (OSINT), analyser les risques de manière structurée (EBIOS), mettre en place des plans de continuité et de reprise d'activité, et améliorer continuellement la posture de sécurité.

Certification et attestation validé

- ✅ **Certification CNIL RGPD** - 6 modules validés (scores : 100%, 100%, 100%, 100%, 100%, 83%)
- ✅ **Attestation SecNumAcadémie (ANSSI)** - 4 modules complétés avec succès (100% chaque module)
- ✅ **Certificat OSINT-FR** - Formation introductive complétée
- ✅ **Certificat ANSSI x Club EBIOS** - Test final réussi (6/6 réponses, 100%)
- ✅ **Attestation SensCyber** - E-sensibilisation validée

Prochaines étapes envisagées

Sur la base de ces formation de bases, les domaines suivants constituent pour moi des approfondissements naturels :

- **Certifications de référence** : CEH (Certified Ethical Hacker), OSCP (Offensive Security Certified Professional), ou GIAC Security Essentials
- **Spécialisation SIEM et SOC** : ELK Stack, Splunk, analyse comportementale, réponse aux incidents
- **Hardening avancé** : CIS Controls, ISO 27001/27002, frameworks de sécurité
- **Pentesting et exploitation** : Metasploit, Burp Suite, techniques avancées d'attaque et défense
- **Cloud Security** : Sécurisation des environnements AWS, Azure, Google Cloud