



Introduction à la cybergdéfense d'entreprise SEC101

Eric DUPUIS^{1,2*}

🔗 Résumé

Ce document fournit les éléments d'introduction au cours SEC101 du CNAM et d'Orange Campus Cyber. Il fait partie du cours introductif aux fondamentaux de la sécurité des systèmes d'information vue sous deux prismes quelques fois opposés dans la littérature : la gouvernance et la gestion opérationnelle de la sécurité. Le cours est constitué d'un ensemble de notes de synthèse indépendantes compilées en un document unique, mais édité par chapitre dans le cadre de ce cours.

Ce document ne constitue pas à lui seul le référentiel du cours CYBERDEF101 (SEC101 du Cnam). Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique partiel à ce cours introductif à la cybergdéfense d'entreprise.

🔑 Mots clefs

SEC101, Cybersécurité, Cybergdéfense, PSSI, ISO27001, Analyse de risques

¹Enseignement sous la direction du Professeur Véronique Legrand, Conservatoire National des Arts et Métiers, Paris, France

²Directeur Orange Campus Cyber

*email : eric.dupuis@lecnam.net – eric.dupuis@orange.com

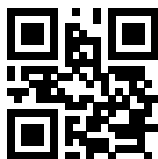
Notes de cours SECOPS 2022-2023

Vérifiez la disponibilité d'une version plus récente de

CourseNotes-FR-SEC101-00-IntroSEC101.doc.pdf sur GITHUB CYBERDEF ¹



Publication en Creative Common BY-NC-ND by eduf@ction



1. <https://github.com/edufaction/CYBERDEF/raw/master/Builder/CourseNotes-FR-SEC101-00-IntroSEC101.doc.pdf>



1. Avant propos

Chaque jour la presse se fait l'écho d'attaques et de piratages informatiques, de divulgations d'informations sensibles ou de fragilités découvertes dans les produits et services numériques. Derrière ces incidents, nous découvrons des menaces certaines fois complexes, des actions criminelles, étatiques ou activistes. Construire des systèmes sûrs, les protéger et les défendre, dans une société où accélérer la digitalisation est devenu un challenge quotidien pour les équipes spécialisées qui luttent contre ces menaces. La cybersécurité est un domaine de mythes et de légendes. Ses activités plongent au plus profond de notre histoire avec des luttes ancestrales entre le méchant et le gentil, le gendarme et le voleur, le corsaire et le pirate, en n'oubliant pas les luttes secrètes entre les espions et le contre-espionnage. Une thématique qui résonne, donc comme un domaine de romans, qui se traduit toutefois par une réalité souvent moins réjouissante pour les équipes chargées de la cybersécurité dans les entreprises. Les métiers de la cybersécurité sont nombreux, pour certains très techniques, d'autres plus fonctionnels, juridiques, ou managériaux.

La cybersécurité est, en effet, une discipline transverse et interdisciplinaire à plusieurs titres. Elle nécessite :

- ▶ de maîtriser les nombreuses techniques et technologies des systèmes d'information ainsi que leurs zones de fragilités ;
- ▶ de maîtriser de nombreuses solutions de sécurité permettant de couvrir, en n'oubliant qu'elles aussi peuvent être fragiles² ;
- ▶ de faire coopérer des métiers et des cultures différentes ;
- ▶ de gérer l'entreprise dans des cadres de conformité souvent complexes et coûteux ;
- ▶ d'intégrer ces démarches en tenant compte des cultures et des pratiques des nombreux métiers de l'entreprise.

Les métiers de la cybersécurité concourent tous à une seule et même mission : « **assurer la continuité de la mission ou du service en préservant le patrimoine de l'entreprise contre toute menace dans l'environnement numérique** ».

Ce sont des métiers de passion, des métiers extrêmement techniques pour partie, fortement marqués par le fonctionnel pour d'autres. S'il est vrai qu'une grande partie des experts du domaine sont issus de formations en informatique ou en électronique, les domaines d'expertises s'élargissent et font naître de nouveaux chemins d'excellence. On trouvera en particulier, des métiers issus du domaine juridique comme celui du Data Protection Officer .

2. Aborder la cybersécurité

La cybersécurité ou la sécurité du numérique³ peut être découverte par de nombreuses voies.

La plus courante est certainement pour les technophiles, l'aventure passionnante de découvrir ce domaine par la technique, et le hacking. Longtemps abordé par le triptyque académique cryptologie, sécurité protocolaire des réseaux, et informatique fondamentale (compilation et théorie des langages, architecture système et bases de données), le domaine s'est vulgarisé avec une forme de gamification de l'apprentissage.

On y trouve en particulier :

2. cf. Certification et Qualification de produits de sécurité et Critères communs ??

3. Historiquement d'autres termes sont utilisés comme Sécurité des Systèmes d'information (SSI) ou Sécurité Informatique





FIGURE 1. Cybersécurité : un domaine holistique

- Les challenges comme les *Capture The Flag (CTF)*, ou les *Defend The Flag (DTF)* qui permettent de mettre le pied dans les techniques et stratégies d'intrusion pour les pentesteurs et auditeurs techniques en herbe ;
- Les bug-bounty qui permettent de se confronter à ses propres limites avec la recherche de failles dans les logiciels avec pour partie des rémunérations au niveau des difficultés ;

Toutefois, un volet peu enseigné, qui ne mobilise pas spécialement les jeunes apprenants du domaine concerne la gouvernance de cette sécurité numérique de l'entreprise.

J'ai souhaité m'intégrer dans une approche globale de la sécurité du numérique pas le biais de quelques processus, en particulier ceux de la sécurité opérationnelle. L'enjeu est de fournir une trame de connaissances pour déployer des actions de cybersécurité en entreprise. Cette trame a pour intention de fournir des points d'accroche et des modèles de compréhension des différentes compétences, actions, et outils du large domaine de la cybersécurité.

Destiné à un public large, cet ouvrage tente d'offrir un niveau de lecture permettant à un expert technique de repositionner sa technicité dans un ensemble plus large, et à un débutant de découvrir de nombreuses facettes du domaine avec quelques éclairages techniques.

La cybersécurité dans une entreprise est une co-activité d'hommes de l'art. C'est aussi un domaine en perpétuelle évolution, soutenu et contraint par des lois, des règlements, des normes, des méthodologies, des technologies spécialisées et en particulier des expertises. Il nécessite pour être efficace d'être orchestré pour maintenir en condition de sécurité une organisation dont le périmètre peut être complexe face à des menaces elles aussi en perpétuelles évolutions.

Il y a de nombreuses manières d'aborder le pilotage de la cybersécurité au sein de l'entreprise, et nombreux ouvrages spécialisés en détaillent les concepts et les méthodologies. Nous avons toutefois



délibérément choisi ici de confronter, si ce n'est corréler, dans un seul support, trois domaines qui apparaissent souvent dans la littérature comme des domaines d'expertise différents : la gestion des risques, la gouvernance de la cybersécurité et la cybersécurité opérationnelle.

Nous avons donc fait ce choix de structurer notre approche suivant le prisme de la cyberdéfense d'entreprise avec une analyse en trois axes majeurs qui résument les difficultés dont relève cette discipline holistique (sch13).

Les 3 axes de la cybersécurité

- ▶ **l'analyse des risques** informatiques sur les actifs les plus sensibles de l'entreprise avec les difficultés d'identifier la sensibilité de ces actifs et les menaces qui pèsent sur l'environnement ;
- ▶ la structuration d'une gouvernance efficace avec des **politiques de sécurité** des systèmes d'information pour des architectures de sécurité de confiance, dans des systèmes d'informations complexes, intégrant des services dans le cloud, des technologies obsolètes et des politiques de sécurité sédimentées ;
- ▶ la construction et l'organisation d'une **sécurité opérationnelle** vue sous un angle d'anticipation et de veille, de détection, et enfin d'alerte et de réponse aux attaques, nécessitant une activité continue avec des ressources de plus en plus expertes et avec des outils plus « pointus ».

2.1 Politiques versus stratégies

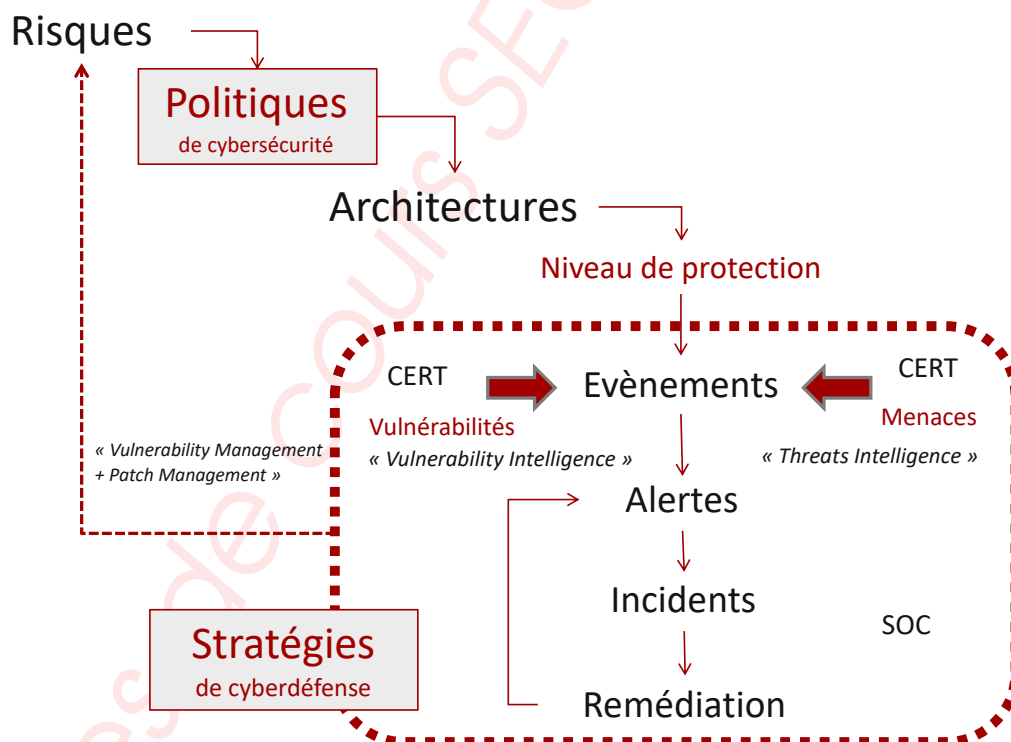


FIGURE 2. Processus Cyber d'entreprise

La figure 2 présente la dynamique avec laquelle nous avons structuré ce document. De **l'analyse de risque**, nous pouvons déduire et/ou modifier des politiques de sécurité adaptées. Sur la base de l'existant, il est alors possible d'adapter ou simplement de mieux utiliser ou configurer les architectures techniques et



organisationnelles pour définir un niveau de protection attendu. Il y a malheureusement toujours un écart entre les mesures de sécurité souhaitées et la réalité des mesures déployées. Que ce soit des défauts de configuration, des délais de mise en place plus longs que prévu, le système n'est que très rarement au niveau décrit dans les éléments de spécification ou les documents d'assurance sécurité. Mesurer ce niveau, analyser les écarts et remédier relève d'un des grands thèmes de la gouvernance sécurité. Il reste à lui seul un consommateur à plus de 30% des charges d'activité de cette gouvernance.

Après avoir défini des **politiques de sécurité** et mesurer leur déploiement dans l'environnement de l'entreprise, il n'en demeure pas moins que l'ennemi est toujours à ses portes et de plus en plus souvent. Il arrive à pénétrer le périmètre de sécurité. Non pas que les barrières et filtre de l'entreprise ne sont plus efficaces mais simplement parce que l'attaquant change plus souvent de stratégie que l'entreprise de politique. La sécurité se doit d'être plus dynamique. L'entreprise doit faire face à des attaquants qui ne raisonnent pas sous forme de politiques d'attaque, mais en stratégie d'action. L'entreprise doit raisonner aussi de la même manière pour se défendre. C'est à ce titre que l'on parle de stratégie de Cyberdéfense. C'est avec des stratégies de « cybersécurité » que nous aborderons les moyens organisationnels et techniques à mettre en place.

Vous trouverez dans ce document une terminologie qui peut être certaines fois éloignée des expressions classiques de la sécurité informatique.

J'ai choisi d'utiliser et mixer sans trop de complexes des termes et concepts issus du monde militaire (renseignement, tenir une position, infiltration . . .) et de nombreux autres issus de l'univers médical (infection, épidémie, comportement).

Ces incursions dans les analogies d'autres champs professionnels, bien que présents pour illustrer certains concepts, n'en demeurent pas moins justifiés par leurs usages de plus en plus répandus dans le monde de la cybersécurité. Par ailleurs, les termes sécurité et cybersécurité pourront être utilisés indifféremment dans le corps de ce document.

2.2 Transformation numérique

La cybersécurité est devenue en quelques années un axe fondamental dans la prise en compte de ces nouveaux risques sociétaux qu'apporte l'informatique au cœur de chaque activité sociale, économique ou politique.

Les transformations digitales d'une grande partie des acteurs économiques apportent de nouveaux risques. Les modifications des conditions d'utilisation des technologies dans les crises comme celle du COVID-19 engendrent aussi des risques globaux réduisant les frontières entre les espaces professionnels et les espaces privés.

Le législateur s'en est saisi depuis bien des années avec de nombreuses réglementations et lois permettant de protéger en particulier, le citoyen et l'Etat.

On notera en particulier dans cette évolution du cadre réglementaire, la protection des données personnelles, mais aussi la protection des systèmes sensibles stratégiques⁴ en lien avec la protection de la nation avec la dynamique de Cyberdéfense soutenue par les différentes lois de programmation militaire depuis 2008. L'entreprise se trouve quant à elle prise en sandwich entre les exigences de l'état et les désirs de liberté que défend le citoyen. Il faut aussi noter que le salarié est souvent un citoyen et son rôle dans la cybersécurité de l'entreprise peut soulever des problématiques complexes⁵.

Se sentir en sécurité dans un monde de transformation digitale c'est bien entendu disposer des moyens

4. Opérateur d'Infrastructures Vitales (OIV) et Opérateur de Services Essentiels (OSE)

5. Lanceurs d'alertes, comportements déviants des utilisateurs légitimes



de se protéger et protéger son patrimoine, que ce dernier soit ou non informationnel, mais aussi de le défendre en continu. Il est de moins en moins accepté de le protéger, en érigeant des murs épais, solides et supposés infranchissables. L'entreprise a besoin de faire circuler rapidement les savoirs, de partager largement des informations entre les salariés, les clients, les citoyens, les fournisseurs...

Il est donc nécessaire de correctement définir les biens vitaux ou essentiels pour y mettre les meilleurs moyens pour les défendre. Par ailleurs comme toute activité protégée et défendue qui peut subir des dommages, il est important de structurer l'activité numérique d'une entreprise ou d'une organisation pour pouvoir fonctionner en mode dégradé, et revenir à la normale en moins de temps possible.

Entre une maîtrise des risques cyber et une capacité de se défendre et réagir, il est nécessaire de disposer déjà d'un bon niveau de protection adaptée aux enjeux du numérique. Il existe de nombreuses définitions de cette cybersécurité.

Pour ma part je vous propose de poser pour la suite de mon propos, une définition simple, qui fait consensus et résume en une pseudo équation la manière dont nous traiterons ce domaine dans ce cours.

Une définition de la cybersécurité :

$$\text{Cybersécurité} \cong \text{Cyberprotection} \oplus \text{Cyberdéfense} \oplus \text{Cyberrésilience}$$

(1)

La cybersécurité est l'enchaînement opéré, organisé, documenté, piloté, optimisé de trois environnements d'actions :

- ▶ **Protéger** l'environnement par les mesures et solutions technologies adaptées au niveau de risque que l'entreprise est prête à prendre ;
- ▶ **Défendre** les actifs les plus sensibles de l'entreprise en surveillant et combattant la menace (y compris l'image de l'entreprise) ;
- ▶ assurer **la continuité et la reprise d'activité** de l'entreprise face à tout incident rendant indisponible tout ou partie d'une fonction essentielle de celle-ci.

La Cybersécurité, est donc, avant-tout, le déploiement de mécanismes de protection des biens et des processus numériques sensibles. C'est avec cette première dynamique que l'entreprise déploie en premier lieu des solutions de sécurité.

Toutefois, malgré ce niveau de protection et souvent les lourds investissements réalisés dans des composants de sécurité périmétrique, l'entreprise peut se faire surprendre avec des attaques contournant ces mesures. Face à ces attaques, l'entreprise découvre que la solidité de l'entreprise n'est pas directement liée aux investissements sur les systèmes de protections. Il lui faut anticiper les menaces, les détecter non seulement sur son périmètre mais aussi dans l'écosystème de l'environnement des menaces potentielles. Ces menaces exploitent des vulnérabilités qu'il convient de détecter en amont.

Malheureusement, malgré ces mesures de protection et de défense qui permet de réagir vite et efficacement, il arrive que des attaques informatiques arrivent à leurs fins. La capacité de l'entreprise à revenir à une situation normale, avec un contexte assaini est un critère dont un chef d'entreprise appréciera la valeur **qu'après un incident**.

Il fut une époque pas si lointaine, où l'analyste consacrait beaucoup de temps à l'évaluation de la probabilité d'une attaque. Aujourd'hui bien que ce paramètre continue quand même à être pris en compte, l'analyste positionne cette probabilité ou vraisemblance à 100% car pour l'entreprise la nouvelle hypothèse n'est pas de savoir "si une attaque va avoir lieu mais plutôt quand elle aura lieu". (cf. figure 3)



Probabilité

P/E	1	2	3	4
1				
2				
3				
4				

Impact

$$R_{\text{isque}} = \frac{\text{Impact}(\text{Evènement, Entreprise}) \times \text{Proba}(\text{Evènement})}{\text{Moyens}(\text{Protection})}$$

FIGURE 3. le cyber-risque

L'ensemble des experts du domaine est globalement en accord sur la posture que doivent prendre les entreprises et les organisations : « Le temps n'est plus de savoir si on sera attaqué ou pas, mais plutôt de savoir quand et comment on le sera », qui concrètement se résume à la certitude que tout incident de sécurité peut se produire.



$$M_{\text{enace}} = \frac{\text{Valeur}(\text{Cible}) \times \text{Fragilités}(\text{Entreprise})}{\text{Moyens}(\text{Attaque}) \times \text{Risques}(\text{Attaquant})}$$

FIGURE 4. La menace : une vision de l'attaquant

Dans les modèles d'analyse de risque et d'évaluation de la cybersécurité, l'analyste se positionne aujourd'hui du point de vue de l'attaquant. Ce regard lui permet de mieux comprendre la menace comme équation duale du risque, mais vu de l'énergie dépensée par l'attaquant et du risque qu'il prend. (cf. figure 4). La menace sera d'autant plus grande que la valeur des actifs visés est importante à ses yeux et que les vulnérabilités sont nombreuses. Elle sera d'autant plus faible que les moyens à déployer sont importants et les risques pris plus élevés.

On notera que la valeur des actifs visés dépend de l'attaquant. Ils ne seront pas les mêmes si l'attaquant est un état, un groupe d'activiste, un groupe criminel. Quand aux vulnérabilités, la majorité des attaques utilise les failles perpétuelles du facteur humain.

3. Sécurité du système d'information

Le système d'information est au coeur de ce « monde digital », et il est le lieu d'activités humaines très denses, permettant à des utilisateurs de réaliser leurs activités, professionnelles ou privées, à l'aide de processus informatiques et de services.

Ces activités doivent de plus en plus faire face à tout un système d'agression orchestré par des attaquants non seulement humains mais aussi « automatiques ». On observe aujourd'hui une multitude de situations critiques, incertaines dont l'occurrence quasi quotidienne provient de phénomènes variés, humains (isolés, en réseau, ...), physiques et/ou technologiques. Parmi ces difficultés qui profitent aux pirates informatiques il y a de nombreuses failles ou fragilités que nous découvrirons, provenant des systèmes du SI sans lesquelles ils ne pourraient exploiter leurs attaques. Ces phénomènes sont une menace pour les



conditions de sécurité du système d'information.

3.1 Gouvernance et conformité

⚙️ chapitre en cours de rédaction, DRAFT non publiable ⚙️

3.2 SECOPS et lutte contre la malveillance

⚙️ chapitre en cours de rédaction, DRAFT non publiable ⚙️

3.3 Les fonctions SSI de gouvernance

Au sein des grandes entreprises, il existe de nombreuses fonctions ou missions pour gouverner, piloter cette sécurité numérique.

- ▶ **Le gestionnaire de risque** ou *Risk Manager* qui porte l'animation de la gestion des risques dans les projets ou dans l'entreprise ;
- ▶ **Le responsable sûreté / sécurité** généralement responsable de la sécurité physique ou sein de l'entreprise (vol, intrusion physique, contrôle d'accès). Il endosse le plus souvent la responsabilité des biens et des personnes ;
- ▶ **L'audit et le contrôle** : Au sein des grandes organisations, il peut exister un service « indépendant » dont la mission est d'auditer et de contrôler les activités des services ;
- ▶ **Les RSSI** : Responsables de la sécurité des Systèmes d'Information ;
- ▶ **Les DSSI** : Au sein des grandes entreprises, les RSSI globaux ne dépendent plus trop de DSI, et possèdent le rang de directeur ;
- ▶ **Le DPO** : la dernière responsabilité apparue dans l'environnement de la sécurité (En France successeur du CIL , Correspondant Informatique et Liberté) (*Data Protection Officer*).

Nous ne présentons rapidement ici que ceux qui seront utilisés directement dans ce document et qui sont fortement en liaison avec la sécurité des systèmes d'information.

3.3.1 Les DSSI et RSSI

Au sein de l'entreprise, il est important que quelqu'un porte la charge de suivre ces conditions de sécurité. C'est le rôle du RSSI (Responsable de la sécurité des systèmes d'information), ou DSSI (Directeur de la sécurité des systèmes d'information). La mission de ce RSSI d'entreprise est de protéger son Système d'Information (SI), de le mettre dans une posture d'amélioration continue tant de son système de protection que de son système de défense. Le RSSI n'est pas seul pour assumer ces missions, à tous les niveaux de l'entreprise, s'organise des fonctions de sécurité tant au sein de la DSI (auquel est souvent rattaché le RSSI), qu'au sein d'autres activités de l'entreprise.

3.3.2 Le DPO

A partir de mai 2018, une responsabilité plus juridique liée à la protection des données a été rendue plus visible avec la nécessité de disposer d'un Data Protection Officer (DPO) en entreprise (Data Protection Officer) héritier en France *Correspondant Informatique et Liberté (CIL)*. Nous n'aborderons pas la fonction, les missions et la dynamique de responsabilité du DPO ici. Il faut toutefois que cette fonction possède de nombreux recouvrements dans la chaîne de gouvernance du risque « informatique » auprès des directions d'entreprise. Orienté vers la protection des données à caractère personnel, le tropisme de la fonction DPO peut conduire certaines structures à oublier des pans importants des risques numériques comme :



- ▶ la protection du patrimoine informationnel. (Espionage industriel).
- ▶ la protection des systèmes d'information contre les risques de ruptures de services (Continuité d'activité)

3.3.3 L'officier de sécurité de défense

Pour les entreprises traitant des informations classifiées de défense ou liées aux contraintes de la classification de l'état, il est indispensable de se doter d'une fonction Officier de sécurité (OS) de défense. Son rôle est de s'assurer de la conformité à l'Instruction Générale Interministérielle IGI 1300 pour le « Confidentiel Défense » et l'instruction Interministérielle II901 pour le « Diffusion Restreinte ».

Nous resterons donc dans le cadre fonctionnel de la Cybersécurité dans son volet protection des Systèmes d'information et gestion des risques numériques. Quand nous aborderons des sujets en forte adhérence avec les dynamiques de la General Data Protection Regulation ou RGPD Règlement général sur la protection des données (GDPR) nous donnerons les liens et les indications adaptés pour les DPO. Par exemple, nous aborderons l'usage des données nominatives collectées et traitées dans les System Incident and Event Management (SIEM), ou celles recueillies sur le DarkWeb etc ...

Consulter le site www.cnil.fr pour parfaire ses connaissances en matière de réglementation européenne sur la protection des données personnelles.

3.3.4 Responsabilités SSI

Le maintien des conditions de sécurité du système d'information des grandes entreprises nécessite un Responsable de la sécurité des systèmes d'information (RSSI) Central ou une fonction semblable rattachée à un niveau plus global de l'entreprise. On découvre ainsi des RSSI rattachés à la direction des risques, la direction générale, au contrôle interne ...

Il n'y pas de rattachement bien défini. La couverture de responsabilité dépend grandement de la taille et de l'activité de l'entreprise, mais aussi de la maturité de celle-ci en matière de gestion de risque et de gouvernance. Il peut y avoir des RSSI par entité, par projet à l'intérieur d'une entreprise. Leur mandat est fixé en fonction des enjeux sécurité de ces entités ou ces projets.

Le fin mot de l'histoire est le « R » de RSSI. Son domaine de responsabilité dépendra de son mandat pour assumer ce rôle de garant d'un environnement « possédant » des bonnes conditions de sécurité. La gouvernance de la sécurité, est au coeur du métier du RSSI. Cette discipline que ce dernier pilote dans l'entreprise se nomme Gouvernance Risques et Conformité (GRC).

La notion de système d'information a profondément évolué ces dernières années. Le périmètre des risques digitaux inclut maintenant des systèmes et services externes à l'entreprise. Beaucoup d'entre eux sous la forme de réseaux sociaux, de services cloud ouvrant par ailleurs le domaine de supervision à la téléphonie avec les smartphones et leurs applications professionnelles ou non.

Bien entendu en fonction de la taille de l'entreprise et de ses enjeux, on peut disposer au sein de l'entreprise de nombreuses personnes ayant une fonction de RSSI.

Le métier est riche et dispose d'un spectre de responsabilité et d'activité très large en terme de poste on y trouve par exemple :

- ▶ **RSSI d'entreprise** : Responsable de la sécurité de sa structure.
- ▶ **RSSI d'un département, d'une organisation intermédiaire** : A l'image d'un RSSI d'entreprise, il assure toute les tâches de gouvernance, il applique et fait appliquer les directives et politique de sécurité



aux équipes du département / division / structure intermédiaire, il déploie les actions décidées dans la chaîne fonctionnelle sécurité

- ▶ **RSSI d'un contrat, d'un projet contractualisé (Security Manager)** : Responsable de la sécurité du déroulement d'un contrat. Souvent lié à un plan d'assurance sécurité, le RSSI contrat se doit d'assurer pour le client ou pour le fournisseur le suivi des exigences de sécurité du contrat.
- ▶ **RSSI Projet** : La responsabilité sécurité couvre le projet, on parle souvent de « security by design ». La responsabilité dans ce type de poste recouvre l'intégration de la sécurité dans le système, le suivi des indicateurs définis (contractuels, ou réglementaires), la remontée des indicateurs de suivi de sécurité à la MOA (Maîtrise d'ouvrage), la prise de décision autour des choix de sécurité
- ▶ **RSSI Produit / Service** : Au delà de ce qui est fait pour un projet, le RSSI produit a en charge de gérer la sécurité opérationnel c'est à dire Maintenir la sécurité de son produit ou de son service.
- ▶ **RSOP** : Le responsable sécurité opérationnelle, est souvent un RSSI dépendant d'une DSI, il est généralement et dans beaucoup de d'entreprise de taille moyenne le RSSI technique. Il assure opérationnellement la mise en place technique des politiques de sécurité et maintien en condition de sécurité l'ensemble de l'environnement informatique. Il est aujourd'hui au coeur de la sécurité opérationnelle face aux attaques et aux crises cyber.

3.4 Maintien en condition de sécurité

Les conditions de sécurité représentent les propriétés fondamentales du SI, appelées : Disponibilité, Intégrité, Confidentialité, Traçabilité (DICT), qui favoriseront le fonctionnement optimisé du SI et éviteront l'avènement d'incidents de sécurité irréversibles ou même gênants pour son fonctionnement. D'un certain point de vue, les conditions de sécurité représentent le paramétrage du SI pour lequel le système fonctionne bien dans des conditions de sécurité « connues et approuvées ».

Ces fameux critères **DICT** ou propriétés de sécurité des systèmes d'information visent les objectifs suivants :

👁 **DISPONIBILITE** : le système doit fonctionner sans faille (arrêt, ou dégradation) durant les plages d'utilisation prévues et garantir l'accès aux services et ressources définies et installées avec le temps de réponse attendu.

👁 **INTEGRITE** : Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.

👁 **CONFIDENTIALITE** : Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

👁 **TRACABILITE** : (ou preuve) : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité tels que :



👁 **AUTHENTICITE** : l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange. On voit aussi dans la littérature la terminologie « critères Authentification, Confidentialité, Intégrité, Disponibilité (ACID) (Authentification, Confidentialité, Intégrité, Disponibilité) ».

👁 **NON-REPUDIATION** : La non-répudiation et l'imputation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Dans un contexte d'activité économique dense et en perpétuel renouvellement, les conditions de sécurité sont aussi en perpétuelle évolution, c'est pourquoi nous parlons d'un cycle de vie vertueux au cours duquel les nouveaux paramètres tirent profit des expériences passées. Ainsi, l'amélioration continue également appelée « lean management » dans d'autres domaines (industrie, ...) travaille elle sur le cycle de vie des conditions de sécurité souvent appelé Plan, Do, Check, Act (Roue de Deming) (PDCA).

Ce cycle de vie doit néanmoins être maîtrisé par le RSSI en place avec ses équipes, il faut co-produire ces conditions de sécurité, cette maîtrise est complexe, fortement dépendante du contexte de l'entreprise, c'est pourquoi elle doit être accompagnée d'une méthodologie rigoureuse et partagée qui constitue le savoir-faire de base du RSSI et de son équipe. Par ailleurs, parmi ces conditions, certaines sont universelles et d'autres propres à chaque entreprise.

Comme le montre le diagramme 5, il est possible aussi d'utiliser un cycle de vie sécurité de type projet, qui se rapproche par ailleurs de la manière dont nous avons structuré ce document.

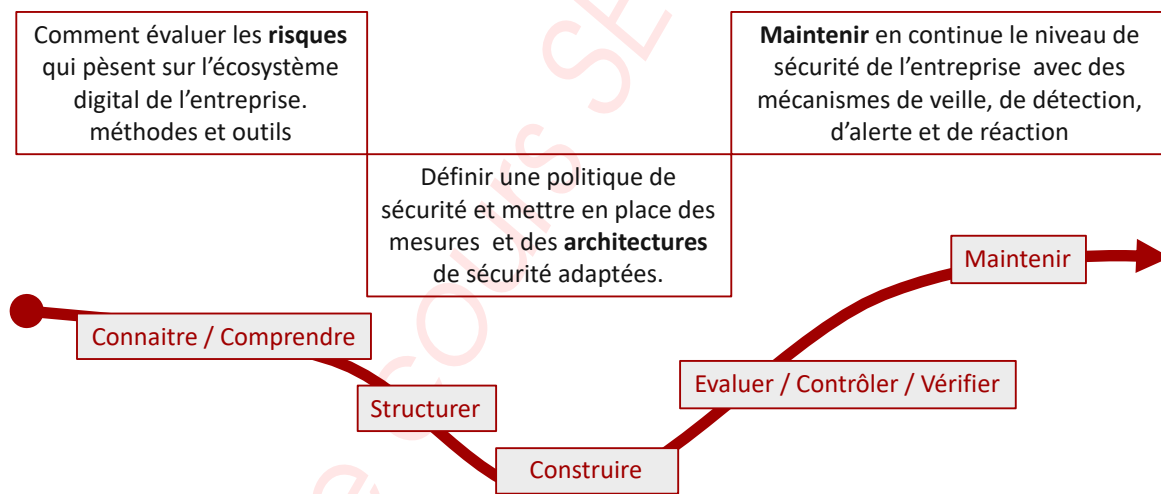


FIGURE 5. Cycle de vie sécurité dans les projets

Dans cette optique, ce cadre méthodologie a été défini par le sous-comité 27 de l'ISO, par l'ensemble de normes ISO 27x. Il s'agit également d'un ensemble de bonnes pratiques, qu'un RSSI peut suivre au travers de trois volets fondamentaux qui constituent les référentiels utilisés pour ce cours sur la cybersécurité. La norme 27001 est en particulier un cadre pour organiser la dynamique de la mise en condition de sécurité de l'entreprise et son maintien dans le temps. Cet environnement que le « RSSI » doit bâtir est le système de management de la sécurité (« SMSI »).

Notre dynamique méthodologique est soutenue dans ce document, par trois cadres normatifs :

- Identifier ses cyber-risques sur la base de méthodologies que l'on retrouve dans l'environnement



ISO/CEI 27001/27005 mais aussi sur la méthodologie Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) de l'ANSSI (Méthode EBIOS RM en particulier) ;

- ▶ Elaborer une politique de cybersécurité sur la base des cadres ISO/CEI 27001 et 27002, en n'oubliant pas les architectures de sécurité et la sécurité des architectures associées ;
- ▶ Détecter en amont des attaques et savoir réagir à ses cyber-incidents en se basant sur ISO 27035 et sur la continuité d'activité avec l'ISO 22301 et 27031.

👁 **Pourquoi des normes dans ce document ?** : L'objectif de ce document, n'est pas de présenter en détail un cadre normatif, mais bien de les utiliser pour ce qu'elles sont : des langages communs permettant d'appréhender une terminologie, des méthodologies, des outils. L'ISO 27001 comporte un grand nombre de normes (plus de 50. . .) qu'il convient de connaître comme outils terminologiques et de référence. Leur maîtrise nécessite une spécialisation le plus souvent demandée pour des métiers de conseil ou d'implémentation pour une certification.

Ces documents définissent un cadre méthodologique et normatif pour définir, créer, élaborer maintenir, améliorer les conditions ou les critères de sécurité pour le fonctionnement du système protégé et surveillé. Ils permettent aux acteurs de l'entreprise évoluant autour du métier RSSI un cadre méthodologique ainsi qu'un « how to » du maintien en conditions de sécurité. C'est en particulier au travers de ces trois axes que la mission de RSSI repose. Le nombre d'entreprises prêtes à accueillir des spécialistes de ce savoir-faire est en forte augmentation car les PME/PMI ont pris conscience que la sécurisation de l'entreprise est devenu primordiale pour « survivre » dans l'écosystème digital de nos sociétés modernes. Les contraintes légales issues de la Loi de Programmation Militaire (Loi de programmation militaire), de la Règlementation pour la Protection des Données Personnelles (RGPD), de la directive NIS nécessitent de disposer d'une vision globale et transverse tant technique, qu'organisationnelle ou humaine de la cybersécurité.

Nous tenterons donc dans le suite du cours, de vous donner des contextes d'usages de ces cadres normatifs indispensables pour aborder la cyberdéfense d'entreprise.

4. Enjeux légaux

Beaucoup d'environnements normatifs sont issus de la pression des différents cadres législatifs sur le marché. Que ce soit avec la pression du grand public ou avec les enjeux stratégiques et économiques des pays, ces lois organisent profondément les modes de gouvernance de la sécurité en entreprise.

4.1 Quelques cadres législatifs d'influence


Parmi les grandes lois qui ont influencées le monde de la sécurité des entreprises ces dix dernières années :

- ▶ En France, le cyberdéfense est largement orientée par les différentes « Lois de programmation militaire » avec des directives nationale de sécurité par grands domaines d'infrastructures vitales.
- ▶ En Europe deux grandes directives ont donné plus de responsabilités aux entreprises dans l'engagement sécurité avec GDPR et NIS qui sont déclinés en droits français via la CNIL, et l'ANSSI. On notera par ailleurs la montée en puissance dans la confiance numérique avec le cadre de certification européen.
- ▶ Aux Etats Unis, le *Cloud security Act*, a bouleversé la vision des risques numériques des états avec les potentielles nuisances liées à l'extraterritorialité de lois américaines




- ▶ En Russie et en Chine, plusieurs lois autour de l'usage d'internet interpellent les entreprises et en particulier celles du numérique sur la protection des données de leurs clients ou utilisateurs de leurs services.

4.2 Le cadre de certification européen

Le règlement établit un cadre européen de certification ⁶ de cybersécurité pour harmoniser à l'échelle européenne les méthodes d'évaluation et les différents niveaux d'assurance de la certification, au sein duquel l'ENISA trouve toute sa place. Les certificats délivrés bénéficieront d'une reconnaissance mutuelle au sein de l'Union européenne (UE).

4.3 Cyberdéfense et loi de programmation militaire

Pour ceux intéressés par les contraintes et cadre généraux de la cyberdéfense au sein des lois de programmation successives (2008, 2013, 2019 ...) il est conseillé d'aller voir sur le site de l'ANSSI. Les différentes LPM ont fait évoluer le cadre réglementaire pour assurer à la France une capacité de défendre la continuité de l'état et des infrastructures vitales du pays (Cf. Opérateurs d'infrastructures vitales) ⁷.

5. Quelques organismes de référence

Pour l'entreprise la cybersécurité est un domaine de nombreux cadres normatifs et réglementaires soutenus bien souvent par contraintes législatives propres à chaque pays.

Cette normalisation et ses réglementations sont riches mais certaines fois complexes. Le plus simple pour s'enrichir de ces savoirs et surtout pour disposer des meilleures informations à la source autant « fréquenter » les sites internet institutionnels des organismes qui sont et continuent à être les points de référence dans le domaine de cybersécurité.

De nombreux services étatiques et de normalisation possèdent des activités dites Cyber dans leur structures :

- ▶ Organismes français : AFNOR, Cert FR, CNIL, HADOPI, ANSSI, DGSE, DGSI, DGA/MI, Commandement de la cyberdéfense, C3N, OCLCTIC, BEFTI ...
- ▶ Organismes internationaux : ISO, ETSI, CERT, Europol, Interpol, ENISA, FIRST ...
- ▶ Organismes étrangers : FBI, CIA, NSA, GCHQ, Unité 8200, Fapsi, The SANS institute, CISA ...

Je vous propose de donner quelques pointeurs par portée sur des organismes de référence du point de vue occidental.

5.1 International et Etats-Unis

Au niveau international, on ne peut éviter les Etats-Unis, un pays qui oeuvre fortement dans le domaine des standards.

5.1.1 Le NIST

Le National Institute of Standards and Technology, ou NIST est une agence du département du Commerce des États-Unis. Son but est de promouvoir l'économie en développant des technologies, la métrologie et des standards avec l'industrie.

6. <https://www.ssi.gouv.fr/entreprise/reglementation/cybersecurity-act-2/le-cadre-de-certification-europeen>

7. <https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/>



- ▶ NIST COMPUTER SECURITY RESOURCE CENTER ⁸
- ▶ NIST INFORMATION TECHNOLOGY LABORATORY ⁹

On notera en particulier les référentiels cryptographiques du NIST et ceux liées à la cybersécurité en particulier avec le *CyberSecurity FrameWork*

5.1.2 SEI : Université de Carnegie Mellon

Le Software Engineering Institute (SEI) est un centre de recherche-développement financé par des fonds fédéraux et placé sous le parrainage du département de la Défense des États-Unis ; son fonctionnement incombe à Carnegie Mellon University. Le SEI travaille avec des organisations pour apporter des améliorations significatives à leurs capacités d'ingénierie logicielle en leur fournissant le leadership technique afin de faire progresser la pratique de l'ingénierie logicielle. Le CERT Division du SEI est l'entité qui fait autorité et cherche à améliorer la sécurité et la résilience des systèmes et réseaux en particulier dans le domaine du logiciel (Carnegie Mellon University - Cybersecurity research).

5.1.3 l'ISO : International Organization for Standardization


L'ISO est une Organisation Internationale participant à l'élaboration de Standards. En ce sens la conformité à une norme a l'avantage d'être reconnue internationalement.

Les normes de la famille ISO 27000 permettent d'organiser et structurer la démarche de la gestion de la sécurité des systèmes d'information, une grande famille de normes avec des positionnement sur l'ensemble du spectre de la sécurité des systèmes d'information :

- ▶ ISO 27001 décrit les processus permettant le management de la sécurité de l'information (SMSI) ;
- ▶ ISO 27002 présente un catalogue de bonnes pratiques de sécurité ;
- ▶ ISO 27003 décrit les différentes phases initiales à accomplir afin d'aboutir à un système de Management tel que décrit dans la norme ISO 27001 ;
- ▶ ISO 27004 permet de définir les contrôles de fonctionnement du SMSI ;
- ▶ ISO 27005 décrit les processus de la gestion des risques ;
- ▶ ISO 27006 décrit les exigences relatives aux organismes qui auditent et certifient les SMSI des sociétés.

Nous aborderons dans le chapitre sur les politiques de sécurité, l'usage de ce cadre normatif dans la gouvernance globale de la cybersécurité au sein de l'entreprise

5.2 Europe

Au niveau européen, le règlement (CE) 460/2004 du Parlement européen et du Conseil du 10 mars 2004 a institué l'Agence européenne chargée de la sécurité des réseaux et de l'information Agence européenne chargée de la sécurité des réseaux et de l'information ENISA ¹⁰. Son rôle est de :

- ▶ Conseiller et assister la Commission et les États membres en matière de sécurité de l'information et les aider, en concertation avec le secteur, à faire face aux problèmes de sécurité matérielle et logicielle.
- ▶ Recueillir et analyser les données relatives aux incidents liés à la sécurité en Europe et aux risques émergents.

8. <https://csrc.nist.gov/>

9. <https://www.nist.gov/itl/fips-general-information>

10. <https://www.enisa.europa.eu>



- ▶ Promouvoir des méthodes d'évaluation et de gestion des risques afin d'améliorer notre capacité de faire face aux menaces pesant sur la sécurité de l'information.
- ▶ Favoriser l'échange de bonnes pratiques en matière de sensibilisation et de coopération avec les différents acteurs du domaine de la sécurité de l'information, notamment en créant des partenariats entre le secteur public et le secteur privé avec des entreprises spécialisées.
- ▶ Suivre l'élaboration des normes pour les produits et services en matière de sécurité des réseaux et de l'information.

5.3 France

En France, la Cybersécurité est pilotée par un organisme dépendant des services du 1er Ministre, l'Agence National des Systèmes d'information (Agence Nationale de la Sécurité des systèmes d'information (ANSSI)). L'ANSSI possède plusieurs rôles de fait. C'est un « régulateur » c'est à dire qu'elle définit des cadres réglementaires pour les entreprises mais c'est aussi une agence qui édicte des préconisations et des guides.

Le site de l'agence [🔗](https://www.ssi.gouv.fr/agence/cybersécurité/ssi-en-france/)¹¹ est riche en information et guide sur la cybersécurité.

Dépendant aussi de l'état, la CNIL [🔗](https://www.cnil.fr/)¹² (Commission National Informatique et Liberté) est une autorité dont la mission est de protéger le citoyen. Avec l'avènement du règlement de protection des données personnelles, la Commission National Informatique et Liberté (CNIL) a vu son pouvoir étendu.

Il faut aussi citer l'AFNOR Association Française de Normalisation (AFNOR), qui relaie en France la normalisation internationale dont l'ISO au delà de ses actions de normalisation purement françaises.

6. Quelques associations et groupements professionnels

A titre d'information, vous trouverez en France aussi quelques clubs et associations historiques de la sécurité de systèmes d'information qui offrent à leurs adhérents des lieux d'échanges très intéressants et publient régulièrement :

- ▶ **Observatoire de la Sécurité des Systèmes d'Information et des Réseaux** (Technique) OSSIR [🔗](https://www.ossir.org/)¹³, association plutôt technique, qui propose de nombreux échanges sur la cybersécurité et existant depuis les années 90.
- ▶ **Club de la sécurité de l'information Français** (Gouvernance) CLUSIF [🔗](https://clusif.fr)¹⁴, association qui propose de nombreux échanges sur la cybersécurité.
- ▶ **Club CyberEdu** (Education) CyberEdu [🔗](https://www.cyberedu.fr)¹⁵, issu des travaux sur la formation des enseignants en cybersécurité de l'ANSSI, l'association regroupe les écoles et les utilisateurs des travaux de CyberEdu.
- ▶ **Club HexaTrust** (Editeurs de produits et services de cybersécurité Français) HexaTrust [🔗](https://www.hexatruster.com/le-club/)¹⁶, regroupe les éditeurs et fournisseurs de services français en cybersécurité.
- ▶ **Club des Experts de la sécurité de l'Information et du Numérique**. (Club de RSSI) le CESIN [🔗](https://www.cesin.fr)¹⁷ est une association regroupant les RSSI d'entreprises, l'adhésion à cette association nécessite un parrainage et vous devez être RSSI.

11. <https://www.ssi.gouv.fr/agence/cybersécurité/ssi-en-france/>

12. <https://www.cnil.fr/>

13. <https://www.ossir.org/>

14. <https://clusif.fr>

15. <https://www.cyberedu.fr>

16. <https://www.hexatruster.com/le-club/>

17. <https://www.cesin.fr>



7. Objectifs pédagogiques

On les nomme « technologies » au collège, « sciences industrielles » ou « sciences de l'ingénieur » au lycée et dans le supérieur. Derrière ces différentes appellations se cachent les mêmes disciplines, utilisées pour comprendre les réalisations techniques qui nous entourent et imaginer celles de demain. Il me semblait donc important d'apporter au lecteur un peu d'information autour des éléments pédagogiques de ce cours orienté vers les sciences et techniques de l'ingénieur cybersécurité. Vous trouverez donc dans ce chapitre quelques éléments sur les compétences, les métiers, le positionnement des activités de la cybersécurité pour protéger et défendre l'entreprise. En effet, ce cours tente d'être une introduction à la éléments de sécurité opérationnelle en cyberdéfense d'entreprise permettant à des acteurs du digital n'ayant pas ou peu de connaissances du domaine de se repérer dans ces activités à large spectre de métiers et de compétences.

Nous y abordons aussi les limites de ce cours ainsi que des recommandations pour profiter du contenu avec plus de facilité pour ceux, en particulier moins familiers du monde de l'informatique et des réseaux.

Je vous engage à explorer le glossaire de l'ANSSI ¹⁸ qui vous permettra de vous familiariser avec les terminologies de la cybersécurité.

7.1 Les compétences à acquérir

A l'issue de ce cours, vous devriez être en mesure de comprendre les mécanismes qui contribuent à la mise en place d'une organisation de cyberdéfense d'entreprise avec les grandes capacités nécessaires. Pour les réaliser avec pleine conscience et efficacité, il est nécessaire de positionner ces activités au sein des autres fonctions digitales d'entreprise.

Les compétences acquises sont de diverses natures, mais globalement vous devriez être en mesure à un niveau de gouvernance et de pilotage :

- ▶ d'analyser les risques numériques pesant sur l'entreprise ou l'organisation ;
- ▶ de mesurer le niveau de sécurité de l'environnement ;
- ▶ d'auditer, conseiller, accompagner le changement ;
- ▶ de mettre en place une gouvernance efficace dans le domaine de la cybersécurité ;
- ▶ de déployer une politique de sécurité informatique et de cybersécurité et appliquer des méthodologies efficaces de renforcement et d'aguerrissement ;
- ▶ de comprendre l'intégration des solutions de sécurité suite à l'analyse de risque ;
- ▶ de gérer des situations d'incident pouvant aller à la crise cyber.

La complexité de l'entreprise, sa taille, sa dynamique de prise en compte des enjeux sécurité, sa culture, l'adhérence ou non aux technologies de l'information nécessitent le plus souvent des projets spécifiques adaptés et très contextualisés. Des sociétés de services assistent les entreprises pour auditer, construire, maintenir la sécurité de l'entreprise. Ce document a aussi pour objectif de fournir au lecteur des clefs de lecture pour encadrer et piloter de telles prestations dans le contexte de l'organisation.

7.2 Métiers et compétences

Il est complexe d'identifier les métiers de la cybersécurité vers lesquels ces compétences peuvent conduire. Il existe plusieurs modèles permettant de classer les métiers de la cybersécurité, et les compétences associées. Pour ma part, j'ai retenu un modèle que j'ai proposé dans le cadre d'une GPEC

18. <https://www.ssi.gouv.fr/entreprise/glossaire>



(Gestion des emplois et compétence) chez un opérateur de services de cybersécurité. Ce modèle est centré sur une classification des outils technologiques utilisés par l'expertise. Issue plutôt de l'expérience, il ne reflète pas les dénominations des différents métiers ou fiche de poste que l'on trouve dans le domaine mais se centre sur les technologies de sécurité vu du côté des opérationnels. Ceci permet de décliner 5 grands domaines d'activité.

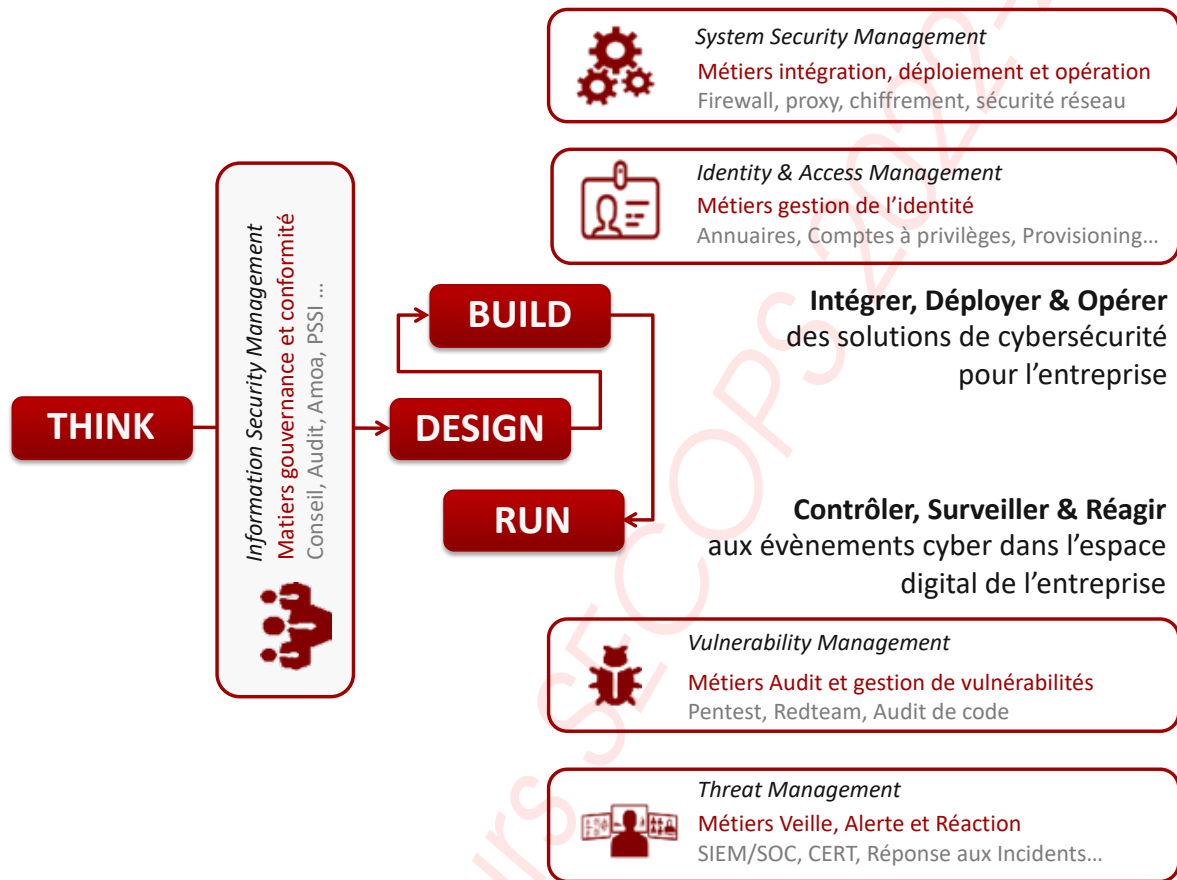


FIGURE 6. les grands domaines de métiers

Il y a en effet une grande différence de métiers, de compétences entre un spécialiste de la gestion des accès qui conduira l'intégration de système d'IAM¹⁹ et un « ethical hacker » qui devra rechercher des scénarii d'attaques potentielles sur un système.

Si vous souhaitez connaître avec plus de détails les compétences nécessaires pour les métiers de la sécurité vous pouvez consulter deux grands sites de référence comme celui de l'**ANSSI** des métiers de la cybersécurité²⁰ ou celui du NIST sur le référentiel NICE Cybersecurity Workforce Framework²¹.

Pour l'ANSSI, la liste de métiers est disponible sur la page du projet SECNUMEDU²²

Par ailleurs, j'ai proposé pour ma part, il y a quelques années dans le cadre d'un enseignement du CNAM, un modèle à cinq domaines qui regroupe globalement des métiers du service utilisant des technologies communes avec des missions similaires et des technologies ou outils communs.

► **Information Security Management** : Les métiers de la gouvernance et de la sécurité de l'information

19. IAM : Identity et Access Management

20. <https://www.ssi.gouv.fr/particulier/formations/panorama-des-metiers-de-la-cybersecurite/>

21. <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework>

22. https://www.ssi.gouv.fr/uploads/2016/05/liste_metiers_ssi_v4_secnumedu_anssi.pdf



et de la sécurité des systèmes d'information, comprenant les métiers du pilotage de la sécurité et du conseil. **Outils typiques** : Logiciels d'analyse de risques (Egerie : Risk Manager), **Méthodologies typiques** : ISO 27005, EBIOS, CRAMM ...

- ▶ **Identity and Access Management** : Les métiers de la gestion de l'identité numérique sont des métiers nécessitant des compétences liées à la gouvernance de l'information et de ses accès mais aussi des compétences techniques liées à la gestion des identités. Fonctionnellement on trouve l'identification (initialisant l'identité de l'utilisateur), L'authentification (de l'utilisateur au système), l'autorisation, (de l'utilisateur à l'accès de la ressource), la gestion de l'utilisateur, et annuaire central d'utilisateurs. **Outils typiques** : Annuaire, Infrastructure de gestion de clefs. **Méthodes typiques** : RBAC, MAC, DAC. ...
- ▶ **System Security Management** : Les métiers du déploiement de la sécurité des systèmes informatiques et réseaux. Métiers de l'intégration, du déploiement et des opérations de solutions de sécurité. Ce domaine regroupe la plus grosse partie des équipes ouvrant dans le domaine de la sécurité de protection périmétrique. On y trouve les expertises des solutions de sécurité. **technologies typiques** : Firewall, Proxy, Bastion ...
- ▶ **Vulnerability Management** : Au coeur d'une partie des métiers de l'audit et de la gestion du maintien en condition de sécurité, la recherche, détection, correction de vulnérabilités (tant techniques qu'organisationnels ou humaines) sont regroupées dans un cadre plus large de la gestion des vulnérabilités. **techniques typiques** : Pentests, Audit applicatifs, audit de fragilités
- ▶ **Threat Management** : Les métiers autour de la gestion de la menace sont nombreux on peut les classer autour de 3 axes : les métiers de la détection, de la veille, l'analyse d'attaque et de la réponse à incident. Chacun de ces axes possède des outillages et des méthodologies particulières. **Méthodes et outils sur la détection** : SIEM, Logs manager..., **Méthodes et techniques de réponse à incident** : forensique, reverse-engineering...

Au delà de ces grands métiers du service, il est possible de positionner dans le cycle de vie des systèmes différents métiers de la cybersécurité. Les cultures, les objectifs, les technologies utilisées sont différentes mais concourent à la même finalité de protection de l'entreprise.

7.3 Compétences et certifications

Se former en cybersécurité, c'est pour celui qui travaille avec vous une certaine garantie de compétences. Dans le domaine de la Cybersécurité, la confiance dans les compétences d'un acteur du domaine se base dans le domaine des services en particulier sur la certification. Dans ces certifications, formes de perfectionnement dans un métier, on trouve généralement des certifications EDITEURS (liés à des produits de sécurité), et des certifications d'associations professionnelles.

Cette dynamique de certification est une manière de compléter les formations initiales. Elles sont assez différenciantes sur un CV dans le monde de l'entreprise en particulier celles qui travaillent dans un environnement international.

7.4 Certifications éditeurs

Nous verrons rapidement dans le chapitre sur les architectures de sécurité, les produits et services technologiques de sécurité. Une grande partie des fonctions de sécurité techniques est opérée par des produits (Logiciels, Appliances, Services SaaS ...). La complexité de ces produits nécessite une formation spécifique pour en exploiter toutes les richesses fonctionnelles. Ces certifications sont par ailleurs souvent fortement préconisées ou même obligatoires pour travailler dans les métiers de l'intégration car elle



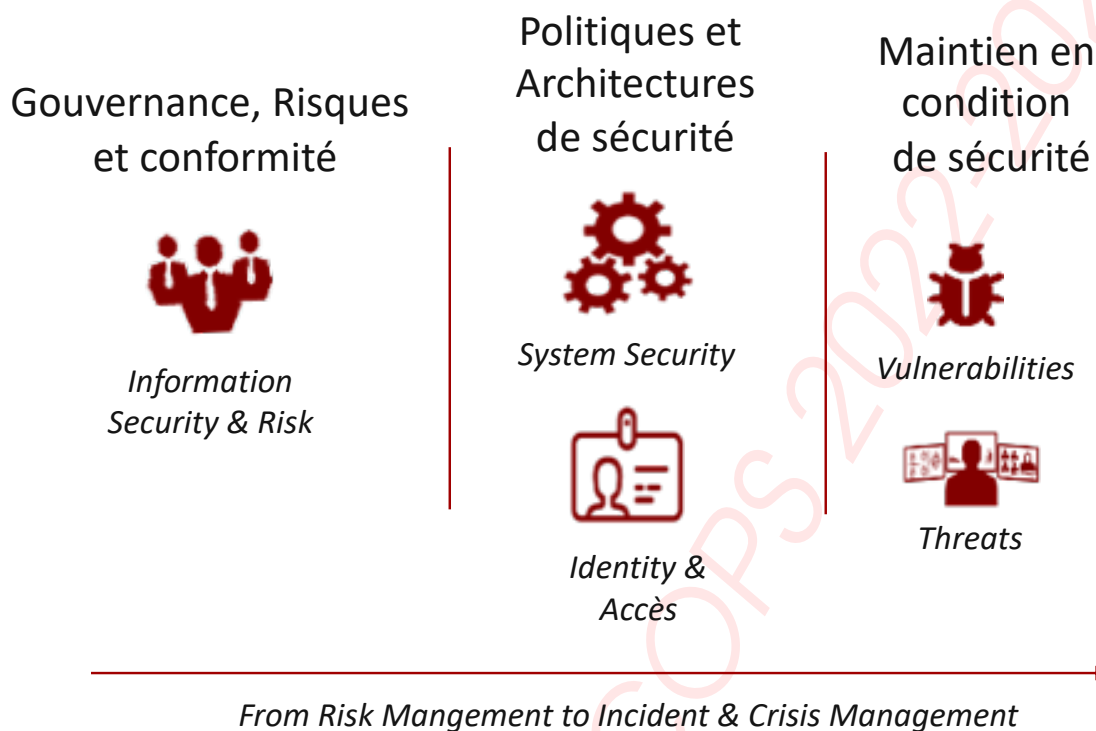


FIGURE 7. les quelques grandes zones de métiers

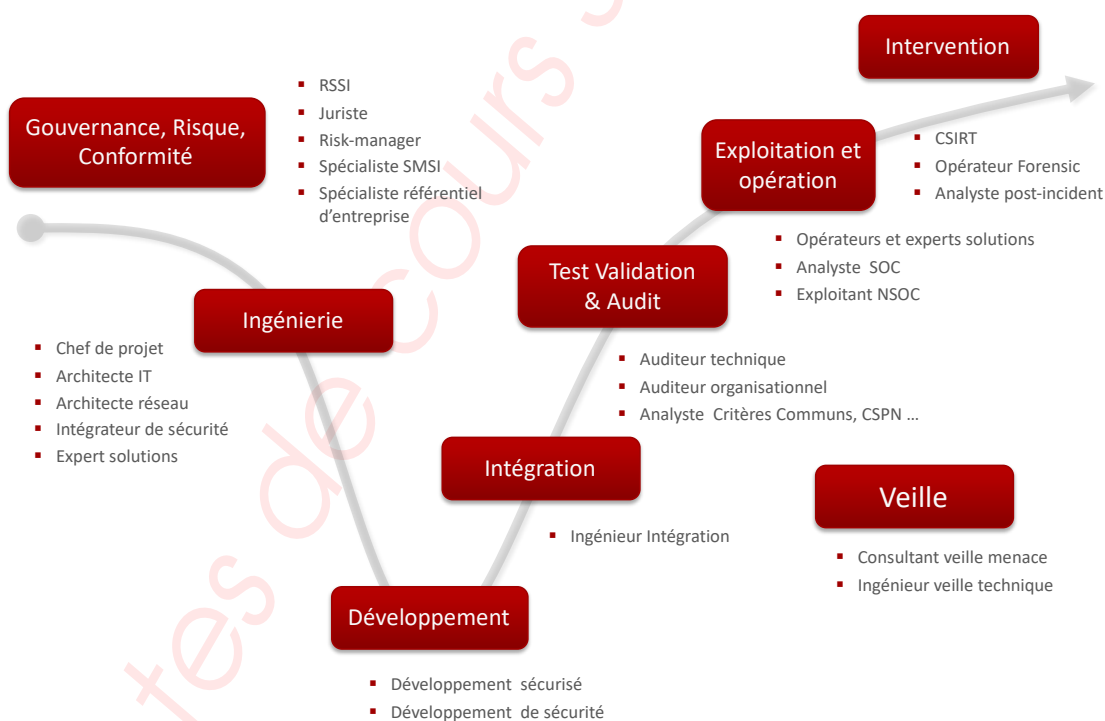


FIGURE 8. les métiers dans le cycle de vie




permettent d'accéder au support des éditeurs. A titre d'exemple, nous pouvons citer deux acteurs connus qui disposent de mécanismes et programme de certifications à leurs produits. Ces certifications peuvent par ailleurs être délivrées par des tiers.

Pour CISCO Certifications de carrière CCNA, CCDA ²³

Pour Microsoft Certifications ²⁴ pour développeurs, administrateurs, architectes solutions, consultants.

7.5 Certifications professionnelles

La validation d'expertise par des certifications professionnelles est assez répandue dans le milieu de cybersécurité et en particulier dans les pays anglo-saxons. De nombreuses certifications existent, portées par des associations professionnelles, des groupes d'experts ou des entreprises de référence. Ces certifications nécessitent le plus souvent en plus de l'examen des années d'expérience et de pratiques prouvées.

ISC ²⁵ *the International Information System Security Certification Consortium* délivre des certifications reconnues et d'excellent niveau de reconnaissance. Les deux principales sont :

- ▶ CISSP : Certified Information Systems Security Professional
- ▶ SSCP : Systems Security Certified Practitioner


ISICA ²⁶ IT Audit, Security, Governance and Risk

sous le nom de *Information Systems Audit and Control Association* cette association professionnelle existe depuis 1967, connue pour son support à COBIT elle propose plusieurs certifications réclamées par les clients.

- ▶ CISA : Certified Information Systems Auditor
- ▶ CISM : Certified Information Security Manager
- ▶ CGEIT : Certified in the Governance of Enterprise IT
- ▶ CRISC : Certified in Risk and Information Systems Control

7.6 Certifications Hacking

Il nous faut citer deux certifications très utilisées dans les métiers techniques de la cybersécurité et accessibles sans expérience professionnelle à prouver.

SANS Institute (SysAdmin, Audit, Network, Security) et le GIAC (Global Information Assurance Certification) ²⁷

- ▶ Cyber Defense ;
- ▶ Penetration Testing ;
- ▶ Incident Response and forensiques ;
- ▶ Management, Audit, Legal ;
- ▶ Developer ;

23. <https://www.cisco.com>

24. <https://www.microsoft.com/fr-fr/learning/certification-overview.aspx>

25. <https://www.isc2.org/Certifications>

26. <https://www.isaca.org/>



27. <https://www.giac.org>



- Industrial Control Systems.

CEH ²⁸ Hacker Éthique Certifié

L'objectif est de savoir comment rechercher les faiblesses et les vulnérabilités des systèmes à partir des mêmes outils et de connaissances qu'un hacker malveillant, mais d'une manière légale et légitime pour évaluer la sécurité du système. La certification CEH se veut par ailleurs indépendante et neutre vis-à-vis des fournisseurs de produits et solutions.

OSCP ²⁹ Offensive Security Certified Professional Une des certifications reconnue pour être une référence dans le domaine des Ethical Hackers de métier. L'OSCP est une certification de l'offensive Security, organisme connu pour le système d'exploitation Kali Linux ³⁰ (anciennement Backtrack), visant à vous fournir une certification attestant de vos compétences au niveau des tests de pénétration (Pentest). Cette certification se passe en ligne avec une dynamique de validation basée sur la mise en pratique des compétences au niveau d'un LAB accessible en VPN, avec le passage de différents niveaux de difficultés.

8. Structure pédagogique du cours

Nous avons abordé le cours sur cheminement basé sur trois pivots :

- Pivot **RISQUES** : Pour défendre son espace cyber c'est-à-dire l'ensemble des produits, services, matériels, données utilisateurs utilisés par l'activité économique de l'entreprise il faut non seulement que celui-ci soit identifié mais que les risques portant sur les éléments le constituant aussi clairement et consciemment soient pris en compte. C'est sur la base d'analyses des risques que sont construits les objectifs de sécurité d'un système. Il est bien entendu que de nombreux systèmes préexistent à une analyse de risque et que les objectifs de sécurité ayant conduit à la construction sont issus de la sédimentation dans le temps de choix technologiques qui sont, par ailleurs rarement formalisés. Ainsi on remarque, que l'activité de l'évaluation des risques, ce qui est appelé en anglais « *risk management* » est porté plutôt par le domaine d'activités dénommé information Security management ou INFOSEC dans les pays anglo-saxons, mais que nous pouvons traduire management de la sécurité de l'information.
- Pivot **ARCHITECTURE du SI**. Architecture de sécurité, défense en profondeur, politique de sécurité, usage du SI, IAM (*Identity and Access Management*). L'analyse sera faite à partir des Politiques de sécurité pour construire ou améliorer la cybersécurité de l'entreprise. Définir des objectifs de sécurité relatifs aux risques, positionner les politiques de contrôle, de filtrage, et de gestion sur l'environnement informationnel de l'organisation pour garantir la protection et la confiance sur les actifs sensibles.
- Pivot **MAINTIEN EN CONDITION de sécurité**. Malgré toutes les précautions pour mettre en confiance un système d'information, il est illusoire d'une part de vouloir tout protéger, mais aussi de penser que les mécanismes de protection résisteront à toutes les agressions. C'est donc en continu qu'il est nécessaire de veiller à la menace, de vérifier que de nouvelles fragilités n'apparaissent pas, de réagir au plus vite en cas de suspicion d'attaque ou de compromission. Cette sécurité continue, dite dynamique est à la base du maintien en condition de sécurité de l'environnement digital de l'entreprise. A titre indicatif, on peut rapidement donner une matrice des classes de métiers

28. <https://www.eccouncil.org/programs/certified-ethical-hacker-ceh/>

29. <https://www.offensive-security.com/information-security-certifications/oscp-offensive-security-certified-professional/>

30. <https://www.kali.org>



associées à chaque pivot. Ceci permettra au lecteur de se focaliser peut être sur un chapitre qui le concerne un peu plus dans son quotidien.

👁 **Les limites de l'exercice :** Ce cours est essentiellement une introduction à la cybersécurité sur son volet gouvernance (politiques et stratégies). Il permet de mettre en perspective les choix techniques, tant de protection et de défense face à une réalité économique, qui nécessite d'adapter protection et défense au niveau de risque. La décomposition sur ces 3 axes est un parti-pris qui évidemment ne couvre pas dans le détail, l'ensemble des processus et actions du domaine de la cybersécurité.

Vu du côté du responsable sécurité, et donc des compétences acquises : Le RSSI se doit de maîtriser les risques de son SI vis à vis des conditions de sécurité, il est un auditeur en mesure :

- ▶ d'analyser les risques à partir de l'analyse des enjeux de l'entreprise, de ses actifs, de son existant, de la menace inhérente ou non à son entreprise ;
- ▶ de les traiter, les accepter ou pas,
- ▶ de proposer les objectifs de sécurité à déployer pour construire les mesures de sécurité.
- ▶ Ceci conduit à l'objectif professionnel de cette partie : Savoir comment démarrer la prise en compte de la sécurité des systèmes d'information dans une entreprise . Il trouvera donc de bons outils théoriques et pratiques dans l'ISO 27005.

👁 **Dynamisme des risques :** Un RSSI ou son équipe conduit les analyses vis à vis de la menace. Il peut être conduit à lancer des audits. Les mesures issues de ces audits permettent de définir sur les mesures en cours sont faibles, inutiles, vulnérables vis-à-vis des objectifs de sécurité. C'est ainsi qu'il est possible de conduire des analyses de risques sur des systèmes existants et de vérifier si les mesures actives sont compatibles avec les objectifs. On peut aussi constater qu'à ce titre une analyse de risque n'est pas figée dans le temps car les menaces ainsi que la sensibilité des actifs évoluent.

Le RSSI se doit de maîtriser les politiques de sécurité des systèmes d'information, la PSSI étant le modèle de référence de façon à :

- ▶ planifier et produire ces conditions de sécurité ;
- ▶ les adapter à l'entreprise ;
- ▶ les mettre en œuvre au travers d'une architecture de sécurité propre à l'entreprise ;

Le lecteur trouvera un référentiel global dans l'environnement de l'ISO 27001 pour travailler autour du système de management de la sécurité.

Au delà de la gouvernance classique que l'on dit « de protection » de la cybersécurité d'entreprise qui se veut un moyen de déployer des mesures de sécurité (préventives, de formation, d'architecture), la sécurité opérationnelle apporte un nouveau lot de mesures et d'outillages liés à l'anticipation, la détection et la réponse aux attaques.

👁 **sécurité Opérationnelle :** Lutte informatique défensive, sécurité dynamique, Cyberdéfense : plusieurs terminologies se côtoient pour évoquer des concepts, techniques, mesures, et méthodes souvent proches.



8.1 Structure

Le cours est donc organisé en trois temps. Chaque temps est une partie qui structure l'ensemble des éléments présentés dans le programme de l'unité d'enseignement dans une dynamique associée à la forme d'enseignement à distance et structurée autour de 3 cours issus des retours d'expérience de professionnels du domaine de la Cybersécurité.

- ▶ **Temps 1** : De l'analyse des risques sur les **actifs les plus sensibles** à la déclinaison des objectifs de sécurité essentiels de l'entreprise ;
- ▶ **Temps 2** : Des objectifs de sécurité retenus à une politique de sécurité **guidant et mesurant** une sécurité implémentée (architectures et systèmes de sécurité et sécurité des architectures et de systèmes d'information) ;
- ▶ **Temps 3** : D'un système d'information **outillé, protégé et défendu** en matière de sécurité à une sécurité opérationnelle **maintenue, vigilante et réactive**.

Ce document regroupe de manière plus détaillée les éléments la troisième partie de l'unité d'enseignement que je nommerai dans la suite dans ce texte : « sécurité opérationnelle », les deux premières parties sont toutefois résumées dans deux chapitres préliminaires, permettant d'intégrer une démarche de sécurité Opérationnelle dans le contexte global de sécurité numérique de l'entreprise.

8.2 Pour s'engager plus rapidement

Du point de vue pédagogique, il est important de noter que vous pouvez aller vous initier au domaine de la sécurité des systèmes d'information avec les travaux de l'ANSSI de la Mallette CyberEDU [↗³¹](https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu). Cette mallette de cours contient les éléments de base pour aborder la cybersécurité et la cyberdéfense d'entreprise.

Ces travaux sont issus d'un marché public de réalisation avec l'Université européenne de Bretagne (qui regroupait 28 établissements d'enseignement supérieur et de recherche) et Orange pour la réalisation de livrables à destination des responsables de formation et/ou des enseignants en informatique.

L'ANSSI met à disposition cette mallette pédagogique qui contient : un guide pédagogique, un cours préparé d'environ 24 heures sur l'enseignement des bases de la sécurité informatique, ainsi que des éléments de cours pour les masters en informatique (réseaux, systèmes d'exploitation et développement). Ces documents, réalisés par le consortium et l'ANSSI, sont disponibles sur le site de l'ANSSI.

8.2.1 Pour le niveau BAC +3

Pour ce niveau la mallette contient un syllabus pour le cours de sensibilisation et initiation à la Cybersécurité ainsi que 4 modules de support de cours.

- ▶ module 1 : notions de base
- ▶ module 2 : hygiène informatique
- ▶ module 3 : réseau et applications
- ▶ module 4 : gestion de la cybersécurité au sein d'une organisation

Un quizz est également à disposition pour permettre d'évaluer les compétences acquises au fur et à mesure de l'avancé des enseignements.

31. <https://www.ssi.gouv.fr/administration/formations/cyberedu/contenu-pedagogique-cyberedu>



8.2.2 Pour le niveau Bac + 5

Pour ce niveau, des fiches pédagogiques par domaine permettent de découvrir :

- ▶ la sécurité des réseaux
- ▶ la sécurité des logiciels
- ▶ sécurité des systèmes
- ▶ l'authentification
- ▶ la cybersécurité au sein des composants électroniques



9. Contributions

9.1 Comment contribuer

Les notes et les présentations sont réalisées sous \LaTeX .

Vous pouvez contribuer au projet des notes de cours CNAM SEC101 (CYBERDEF101). Les contributions peuvent se faire sous deux formes :

- ▶ Corriger, amender, améliorer les notes publiées. Chaque semestre et année des modifications et évolutions sont apportées pour tenir compte des corrections de fond et de formes.
- ▶ Ajouter, compléter, modifier des parties de notes sur la base de votre lecture du cours et de votre expertise dans chacun des domaines évoqués.

Les fichiers sources sont publiés sur GITHUB dans l'espace : (edufaction/CYBERDEF) ³². Le fichier Tex/-Contribute/Contribs.tex contient la liste des personnes ayant contribué à ces notes.

Le guide de contribution est disponible sur le GITHUB. Vous pouvez consulter le document **SEC101-C0-Contrib.doc.pdf** pour les détails de contributions.

32. <https://github.com/edufaction/CYBERDEF>



Table des matières

1	Avant propos	2
2	Aborder la cybersécurité	2
2.1	Politiques versus stratégies	4
2.2	Transformation numérique	5
3	Sécurité du système d'information	7
3.1	Gouvernance et conformité	8
3.2	SECOPS et lutte contre la malveillance	8
3.3	Les fonctions SSI de gouvernance	8
3.3.1	Les DSSI et RSSI	
3.3.2	Le DPO	
3.3.3	L'officier de sécurité de défense	
3.3.4	Responsabilités SSI	
3.4	Maintien en condition de sécurité	10
4	Enjeux légaux	12
4.1	Quelques cadres législatifs d'influence	12
4.2	Le cadre de certification européen	13
4.3	Cyberdefense et loi de programmation militaire	13
5	Quelques organismes de référence	13
5.1	International et Etats-Unis	13
5.1.1	Le NIST	
5.1.2	SEI : Université de Carnegie Mellon	
5.1.3	I'ISO : International Organization for Standardization	
5.2	Europe	14
5.3	France	15
6	Quelques associations et groupements professionnels	15
7	Objectifs pédagogiques	16
7.1	Les compétences à acquérir	16
7.2	Métiers et compétences	16
7.3	Compétences et certifications	18
7.4	Certifications éditeurs	18
7.5	Certifications professionnelles	20
7.6	Certifications Hacking	20
8	Structure pédagogique du cours	21
8.1	Structure	23
8.2	Pour s'engager plus rapidement	23
8.2.1	Pour le niveau BAC +3	
8.2.2	Pour le niveau Bac + 5	
9	Contributions	25
9.1	Comment contribuer	25

Table des figures

