

Enjeux pédagogiques du cours SEC 101

Eric DUPUIS^{1,2*}

🕒 Résumé

Ce document fournit les éléments du contexte pédagogique de l'unité d'enseignement SEC101. Il introduit les enjeux pédagogiques qui ont été à l'origine de la constitution de ce cours. Il cerne les connaissances cybersécurité acquises au titre de cet enseignement ainsi que les limites de celles-ci.

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 final unique.

Ce document ne constitue pas à lui seul le référentiel du cours. Il compile des notes de cours mises à disposition de l'auditeur comme support pédagogique.

🔑 Mots clefs

Pédagogie, Organisation, Méthode

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

²RSSI Orange Cyberdefense

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

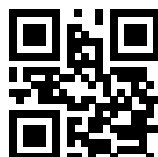
DRAFT NOTES S2 - 2020

Vérifiez la disponibilité d'une version plus récente de

SEC101-C0-Pedago.doc.pdf sur GITHUB CYBERDEF [↗](https://github.com/edufaction/CYBERDEF/raw/master/Builder/SEC101-C0-Pedago.doc.pdf)¹



2020 eduf@ction Publication en Creative Common BY-NC-ND



1. <https://github.com/edufaction/CYBERDEF/raw/master/Builder/SEC101-C0-Pedago.doc.pdf>



1. Objectifs pédagogiques

Il me semblait important d'apporter au lecteur un peu d'information autour des éléments pédagogiques de ce cours . Vous trouverez donc dans ce chapitre quelques éléments sur les compétences, les métiers, le positionnement des activités de la cybersécurité. 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.

1.1 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 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.

1.2 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 (Gestion des emplois et compétence) dans 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.

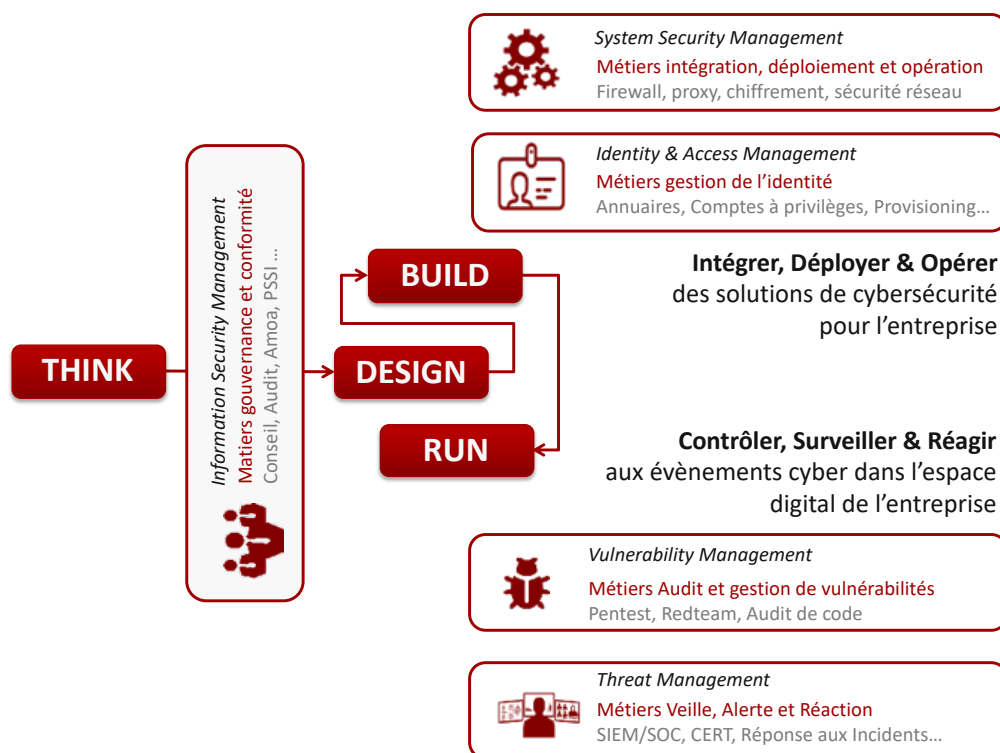


FIGURE 1. les grands domaines de métiers

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'IAM² 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 cybersécurité³ ou celui du NIST sur le référentiel NICE Cybersecurity Workforce Framework⁴.

Par ailleurs, j'ai proposé pour ma part, il y a quelques années dans 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.

2. Identity et Access Management

3. <https://www.ssi.gouv.fr/particulier/formations/profils-metiers-de-la-cybersécurité/>

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



- ▶ **Information Security Management** : Les métiers de la gouvernance et de la sécurité de l'information 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 de réponse à incident** : Forensic, 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.

1.3 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.



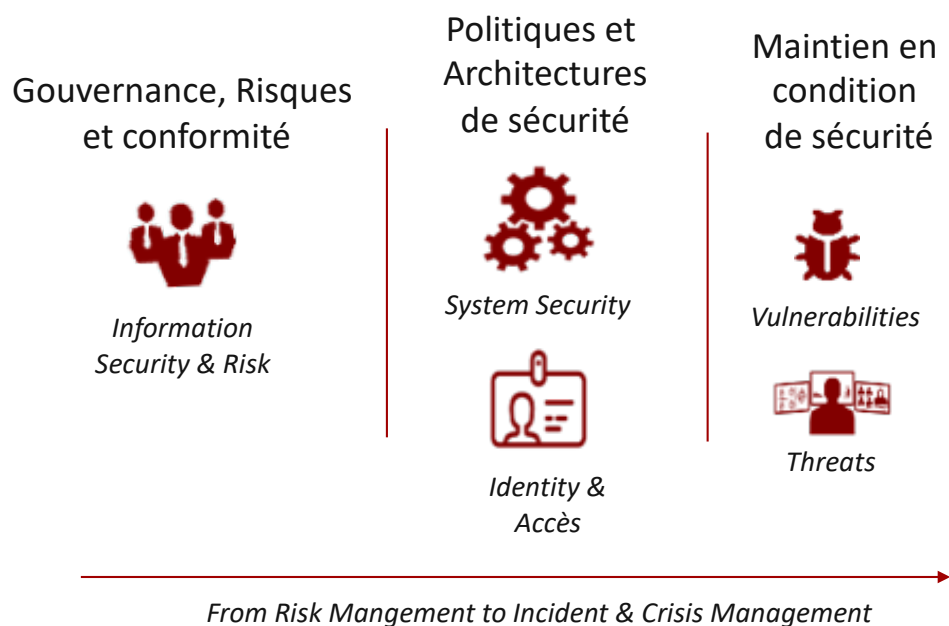


FIGURE 2. les quelques grandes zones de métiers

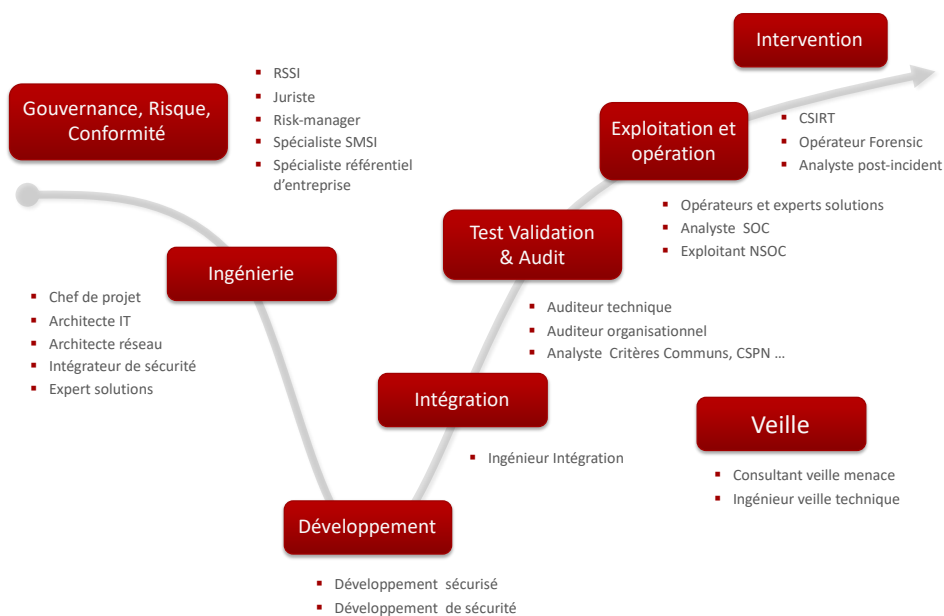


FIGURE 3. les métiers dans le cycle de vie



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

1.4 Certifications éditeurs


Nous verrons 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 obligatoires pour travailler dans les métiers de l'intégration car elles permettent d'accéder au support des éditeurs. A titre d'exemple, nous pouvons citer deux acteurs connus qui disposent de mécanismes et programmes de certifications à leurs produits. Ces certifications peuvent par ailleurs être délivrées par des tiers.

Pour CISCO Certifications de carrière CCNA, CCDA ⁵

Pour Microsoft Certifications ⁶ pour développeurs, administrateurs, architectes solutions, consultants.

1.5 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 ⁷ *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

ISACA ⁸ 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

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

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

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

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



- ▶ CRISC : Certified in Risk and Information Systems Control

1.6 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) ⁹

- ▶ Cyber Defense ;
- ▶ Penetration Testing ;
- ▶ Incident Response and Forensics ;
- ▶ Management, Audit, Legal ;
- ▶ Developer ;
- ▶ Industrial Control Systems.

CEH ¹⁰ 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 ¹¹ 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 ¹² (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.

2. Structure pédagogique du cours

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

- ▶ Pivots **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 pris en compte. C'est sur la base d'analyses des risques que sont construits les objectifs de sécurité

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

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

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

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



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 ne sont, par ailleurs rarement formalisés. Ainsi on remarque, que l'activité de l'évaluation des risques, ce que appelle 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 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.

👁 **Dynamicité 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, Cyber-défense : plusieurs terminologies se côtoient pour évoquer des concepts, techniques, mesures, et méthodes souvent proches.

2.1 Structure du cours


Le cours est donc organisé en 3 temps. Chaque temps est un module 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 d'experts du domaine de la Cybersécurité.

- ▶ **Temps 1** : De l'analyse des risques à la déclinaison des objectifs de sécurité sur les essentiels de l'entreprise ;
- ▶ **Temps 2** : Des objectifs de sécurité 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 3^{ème} partie de l'unité d'enseignement que je nommerai pour la suite dans ce texte VAR : Veille / Alerte / Réponse , les deux premières parties sont toutefois résumés dans deux chapitres préliminaires, permettant de positionner la démarche VAR dans un contexte global.

2.2 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 ¹³ . Cette mallette de cours contient les éléments de base pour aborder la cyberdéfense d'entreprise.

Ces travaux sont issus d'un marché public de réalisation avec l'Université européenne de Bretagne (qui regroupe 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.

2.2.1 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.

2.2.2 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

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



3. Contributions

3.1 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) ¹⁴. 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.

3.2 Les contributeurs/auteurs du cours

Les auteurs des contributions sont :

3.2.1 Années 2020

- ▶ **David BATANY** (Contributeur LATEX) : BOTNET
- ▶ **Charly Hernandez** : User and Entity Behavior analytics, UEBA
- ▶ **Florian PINCEMIN (Orange)** : SIEM en quelques mots

3.2.2 Années 2019

- ▶ **François REGIS** (Orange) : CyberHunting

3.2.3 Années 2018

- ▶ **Julia HEINZ** (Tyvazoo.com) : ISO dans la gouvernance de la cybersécurité

¹⁴. <https://github.com/edufaction/CYBERDEF>



Table des matières

