# Les besoins de formation en cyber sécurité - Enquête auprès des entreprises

Patrick Lallement, Germain Malnoury, Alain Corpel
Université de Technologie de Troyes
Institut Charles Delaunay (UMR CNRS 6281)
10004 Troyes Cedex - France

21 mars 2014

## 1 Introduction

Dans le cadre du projet européen 2CENTRE [1], une étude a été réalisée pour évaluer les besoins en formaiton en cybersécurité dans les entreprises en général, qui embauchent (ou sont sensées le faire) des compétences dans le domaine. L'enquête menée s'est déroulée sous forme d'interviews soit individuelles soit en groupe. Cet article de synthèse (qui n'est pas le livrable final officiel du projet) est structuré de la manière suivante. On présente la méthodologie suivie (partie 1). La partie 2 synthétise les interviews. La partie 3 propose une traduction des besoins en termes de contenus d'enseignement.

## 2 Méthodologie d'enquête

### 2.1 Typologie des entreprises

Il s'agit ici essentiellement des entreprises susceptibles d'embaucher des compétences en sécurité ou du moins d'être sensibilisées au cyber risque. Cette topologie doit permettre de définir des profils et cibler des questions spécifiques.
L'idée retenue au départ est de réunir des groupes de 4 ou 5 compétences (RSSI) et de leur soumettre des scénarios préparés en leurs posant des questions de manière interactive pour les confronter à des connaissances qui manquent, ce qui permet de leur point de vue de les sensibiliser.
Il faudra notamment évoquer comment on peut apporter une culture cybercriminalité (le processus) à des gens qui ont d'abord une formation SSI : gestion des incidents, prise en compte des facteurs d'impact (assurances), infractions informatique & liberté, accès à la preuve, gestion des perquisitions, interactions processus SSI et cybercriminalité.
Le Type 2 réunit ceux qui gèrent la fraude ; ils n'ont souvent pas de formation dédiée.
Le type 5 concerne les agents privés de recherche, enquêteurs particuliers, ils ont souvent de mauvaises pratiques (non respect des données relatives à la privée

1. financement DG Home (2010-2013)

notamment).
Le type 7 concerne les avocats. Pour les affaires civiles, tout se fait de manière dématérialisée. Les avocats sont victimes potentielles.
La typologie de ces groupes est donnée tableau 1, ainsi que les interlocuteurs identifiés a priori.

| Type | Entreprises | Interlocuteurs |
|---|---|---|
| 1 | Industries en général | RSSI |
| 2 | E-commerce, banques, opérateurs | Brigade de répression des fraudes |
| 3 | Production composants TIC | Responsables |
| 4 | Secteur cyber défense | Min. défense |
| 5 | Administrations | ANSSI |
| 6 | Acteurs privés de la sécurité | CNAPS |
| 7 | Avocats | Cabinets |

TABLE 1 – Typologie des entreprises

## 2.2 Approche des entreprises

Il ne faut pas aborder de front le sujet du traitement des incidents qui peut provoquer une perte de confiance des interlocuteurs (le sujet pouvant être sensible à très sensible pour le type 2 ou le type 4). Pour ces raisons, il faut traiter du domaine de la cyber sécurité en général (risques, protections, recrutements, compétences recherchées, évolution des métiers, veille) et aborder le cas de la gestion des crises quand c'est nécessaire.
Il s'est avéré difficile de réunir des interlocuteurs pour les raisons suivantes :

- Forte dispersion géographique : type 3 notamment qui concerne souvent des PME spécialisées
- Forte concurrence entre acteurs (notamment le domaine défense et sécurité)

Le type 1 et le type 2 ont permis d'inviter ensemble plusieurs RSSI et de leurs poser des questions relativement à leurs secteurs.
Pour le type 3 (domaine TIC) ont été interrogées une entreprise qui développe des systèmes embarqués, une entreprise qui effectue des développements web, une entreprise opérateur du cloud. Les résultats seront à corréler avec les observations des entreprises qui externalisent leurs développements.
Pour le type 4 (défense) ont été interrogés : le ministère de la défense ainsi que deux grandes entreprises du secteur.
Pour le type 5 (administration) ont été interrogés les DSI de deux conseils généraux (CG), d'une collectivité, une Caisse d'Allocation Familiales (CAF), et le ministère des finances (Direction Générale au Trésor).
Pour le type 6, très hétérogène, le Conseil National des Activités Privées de Sécurité (CNAPS) Grand Est (Metz) a été interviewé.
Pour le type 7, un cabinet d'avocat spécialisé dans le droit des TIC a été interviewé ainsi qu'un cabinet d'avocats de petite taille, spécialisé surtout dans le droit des entreprises.

Selon le type d'entreprises, les questions ont été plus ou moins techniques, plus ou moins stratégiques. Les questions abordées en général portent sur :

– Le recrutements des compétences en sécurité : besoins, niveaux, profils, sources, difficultés
– Les nouveaux besoins, nouveaux métiers
– Les problématiques d'échange de données, de confidentialité
– La gestion des incidents de sécurité (organisation, enquêtes, procédure juridique).
– Le développements des outils (applications web notamment) : niveau de sécurité requis ? Externalisation ? Retour d'expérience.
– La veille : menaces, usages, comportements.

Le tableau 2 cible plus précisément la pertinence des questions.

| Questions | T1 | T2 | T3 | T4 | T5 | T6 | T7 |
|---|---|---|---|---|---|---|---|
| Recrutements | X | X | X | X | X | - | - |
| Nouveaux métiers | - | - | - | X | - | - | - |
| Prot. données | X | X | - | - | X | X | X |
| Gestion des incidents | X | X | - | - | - | - | - |
| Développents sécurisés | X | X | X | - | X | - | - |
| Veille | X | X | - | X | - | - | - |

TABLE 2 – Typologie des questions en fonction des types d'entreprises

# 3 Synthèse des résultats

Plutôt que de reprendre un à un les différents types d'entreprises nous présentons une synthèse relative aux questions qui se posent soit côté 2Centre soit côté entreprise afin de mieux identifier les besoins, les risques, les pistes d'amélioration.

## 3.1 Recrutements

De manière générale et assez unanime, les entreprises expriment des difficultés à recruter. Les raisons sont diverses mais peuvent cumuler leurs effets.
L'état affiche un recrutement important pour ses propres besoins centraux, ce qui dans un contexte de déséquilibre entre la demande et le nombre de diplômés (seulement 25% des besoins seraient couverts d'après l'ANSSI (Agance Nationale de la Sécurité des Systèmes d'Information) tend à stresser le marché du travail. Pour certaines entreprises qui ont des obligations de sécurité, cela conduit à adapter sa stratégie de recrutement en débauchant d'abord en interne (service DSI par ex.) mais aussi chez les prestataires de services (qui de leur côté peuvent pratiquer la réciprocité).
Certaines entreprises recherchent plutôt des compétences expérimentées, ce qui complique encore le processus de recrutement. Les séniors ont plus de capacité à trouver des postes à leur convenance ce qui augmente l'instabilité des personnels. Dans le cas des grandes entreprises, cela impose d'assurer des parcours professionnels sur le long terme.
Les processus d'embauche des administrations sont compliqués et donc décourageants alors que les besoins existent comme partout ailleurs, surtout dans un contexte de décentralisation accrue et de modernisation des services. Cela s'aggrave encore quand les postes se situent en province. Les salaires sont aussi peu

motivants.

## 3.2 Les compétences et les métiers de la cyber-sécurité

Les compétences concernent d'abord les aspects fonctionnels et techniques. Le niveau de référence est le plus souvent bac + 5. Beaucoup d'entreprises manifestent leur difficulté à trouver des jeunes diplômés opérationnels sur certains sujets techniques, surtout au niveau applicatif (annuaires par ex.). La compétence technique nécessaire en sécurité est souvent considérée comme supérieure à celle attendue dans la production en général. Beaucoup de gens se proclament des cyber spécialistes et proposent du conseil dans le domaine mais le plus souvent n'ont pas le fond technique pour être crédibles.
Dans les administrations, le métier de RSSI (Responsable SSI) n'est pas reconnu dans le référentiel utilisé dans les concours mais une évolution est probable. Plusieurs conseils généraux envisagent de créer un poste de RSSI (actuellement ce sont les DSI qui s'en chargent).
Plusieurs acteurs concernés par la cyber défense mènent actuellement une réflexion pour définir un référentiel des métiers, une gestion des parcours sur le long terme.
Dans le cadre de ce qui existe dans le Répertoire Opérationnels des Métiers et des Emplois (ROME), 15 profils sont proposés :

1. **Architectes** : celui qui conçoit et a autorité (donc droit de veto) sur les architectures ayant comme point d'application : les infrastructures, les applis, les produits.
2. **Experts** : l'expertise correspond à un niveau senior et porte sur un domaine d'application ; les chercheurs / docteurs correspondent à ce profil
3. **Développeurs** : cela correspond aux aspects hardware, micro-électronique, software (ils doivent être capables de corriger un logiciel, cela concerne à la fois les aspects sûreté de fonctionnement et sécurité, (être capable de développer du code qui devra être certifié pour l'aéronautique par ex.)
4. **Intruders** : pen testeurs, agissent au niveau Forensic ; ce sont souvent des non diplômés (voire bac +3, il existe maintenant des licences pro sur le sujet) ; ils correspondent à des gens passionnés, difficiles à gérer, volatiles, il faut donc les encadrer intelligemment, les faire adhérer à une cause.
5. **Opérateurs** : dans un SOC [2], ils surveillent les alertes (astreintes), doivent prendre les bonnes décisions
6. **RSSI** : en exploitation, dans un centre informatique, auprès du manager d'un SOC.
7. **Analystes** : ils agissent en amont et font du veille (ici assimilable à du renseignement) sur la menace, les failles au niveau opérationnel
8. **Formateurs** : cela suppose des cours mais aussi des exercices et de la simulation, de mettre les élèves en situation avec de vraies architectures, de faire des tests d'intrusion avec de vrais incidents, afin d'être en mesure de gérer les crises

2. Security Operating Center

9. **Juristes** : dans le domaine cyber (inclut l'international), dans le domaine des affaires (assurances)
10. **Auditeurs** : ils interviennent en amont au niveau certification, conseil, conformité
11. **Post-auditeur** : ils interviennent au niveau de la gestion de crises, pour proposer un plan de reconstruction, cloisonner le hacker, définir les modes de réactivité
12. **Gestionnaires de crises** : agissent au niveau PRA/PCA.
13. **Consultants SSI** : contrairement aux auditeurs, ils ne sont pas au niveau de la norme mais du conseil de haut niveau
14. **Experts métiers connexes** : suffisamment compétents en cyber mais avant tout spécialistes d'un type de système, par ex. les architectures de systèmes SCADA[3], les systèmes d'armes ; ils connaissent d'abord les applications métiers et ils ont ensuite une approche sécurité
15. **Techniciens support SSI** : agissent au niveau maintenance, plutôt niveau licence pro mais avec une VAE ils devront s'intégrer dans la grille Thales qui commence en principe à Bac+5

Cette typologie, visant à cartographier les compétences (catalogue, mise en cohérence des fiches ROME) s'accompagne de certaines recommandations :

- Il faut définir les métiers sensibles vis-à-vis de la sécurité nationale
- Il faut restreindre les accès aux formations afin de ne pas livrer des informations stratégiques à des gens ne pouvant être habilités au niveau défense nationale française
- Il faut définir des passerelles entre les différents métiers de la sécurité
- Il faut traiter le cas des carrières des non diplômés (intruders par ex.)

## 3.3 Echanges de données / protection des données

Cela concerne surtout les administrations territoriales qui interagissent avec d'autres administrations, d'autres services (sociaux par ex.) mais aussi avec des entreprises privées (transport par ex.) et des particuliers (domaine social). Les préconisations de l'administration centrale dans le cadre de la modernisation des services publiques sont souvent considérées comme incomplètes et incohérentes. Quelques administrations territoriales comme le CG10 ont pris l'initiative de développer selon leurs besoins.
Les ministères suivent les recommandations de l'ANSSI. Elles limitent strictement l'usage des smartphones et des clés USB. Les échanges se font avec vérification d'intégrité. Les préconisations supposent d'uniformiser les OS des postes de travail et de limiter les applications en fonction des droits.
Le monde de la sécurité privée est un cas particulier. Il n'existe aucune sensibilisation et aucun contrôle sur la conservation des données.
Les avocats sont sensibilisés via le réseau des avocats, mais hormis les cabinets spécialisés dans les TIC, il semble que la culture de la dématérialisation reste faible.

3. Supervisory Control and Data Acquisition

## 3.4 Traitement des incidents de sécurité

Il y a plusieurs aspects :
- La détection
- La gestion de crises (processus SSI)
- L'enquête, à la fois enquête interne, dépôt de plainte et enquête externe (processus cybercriminalité)

Les politiques suivies sont très diverses. Les ministères ont des systèmes de détection d'intrusion à base de logs et les signalements et les investigations sont du ressort de l'ANSSI. Les administrations territoriales n'ont pas vraiment de moyens de détection, elles ont donc peu d'incidents à signaler.
Les entreprises dans le périmètre de la défense ne s'expriment pas sur le sujet mais ce sont celles qui sont les plus sensibles à la protection et à la détection et qui mettent le plus de moyens (SOC par ex.). Les préconisations sont faites par l'ANSSI, les enquêtes judiciaires sont du ressort de la Direction Centrale du Renseignement Intérieur (DCRI).
On peut noter que ce secteur a besoin de formation qui mette en situation les décideurs pour gérer des crises et les amener à prendre les bonnes décisions. Cela concerne les métiers opérateurs de SOC, de gestionnaire de crises, et à un degré moindre de RSSI et de post-auditeur. Cette formation est à mettre en perspective avec le besoin d'intruders. Les entreprises privées qui passent contrat avec un opérateur de cloud pratiquent de plus en plus des tests d'intrusion afin de vérifier leur niveau de sécurité. De plus, une réflexion est actuellement en cours sur un changement de paradigme quant aux tests de sécurité des systèmes (des composants de sécurité en général). Dans le domaine de la cyber-défense, les tests d'intrusion (et les tests de sécurité en général) ont un caractère systématique et donc déterministe qui se suffit plus. L'objectif est de se rapprocher de plus en plus des conditions réelles (à base de connaissances des attaques du passé) en se plaçant du côté de l'attaquant. Dans un tel contexte, le rôle des intruders prendra de l'importance.
En matière de gestion des incidents les entreprises privées ont des comportements très hétérogènes car selon leurs secteurs d'activité, leur type d'activité (B2B, B2C) [4], leurs obligations, les menaces (et donc les risques) sont différents. Plusieurs critères interviennent pour gérer les incidents : l'image de marque (surtout dans le cas B2B), le niveau de dommage (chiffrage de la fraude par ex.), le seuil de tolérance défini au niveau PSSI. La cellule de crise doit décider de la suite à donner en évaluant tous ces critères. Les aspects juridiques sont ici importants mais les entreprises ne cherchent pas de compétences spécifiques (techniques ou juridiques) en cyber criminalité. Ce sont les cellules juridiques existantes qui sont mises à contribution.

## 3.5 Développements sécurisés

La plupart des entreprises se plaignent aujourd'hui du développement sécurisé. Beaucoup de services en lignes sont sous-traités. Les entreprises sont souvent des PME, voire des TPE, à l'étranger, avec des durées de vie aléatoires. Les cahiers des charges ne mentionnent pas souvent la sécurité, mais quand ils le font, les développements sont insuffisants. Les formations en développement logiciel sécurisé sont faibles. Quand le besoin existe, les développeurs sont formés

4. Business to Business, Business to Consumer

sur le tas. Dans le cas des systèmes embarqués les entreprises doivent respecter des contraintes fortes et le logiciel doit être certifié (cas de l'aéronautique par ex.).
Dans le secteur de la cyber défense, le point noir se situe dans la sécurisation des systèmes SCADA, notamment dans la reprogrammation sécurisée du système après incident. SCADA est une boite à outils qui est configurée et paramétrée pour un processus industriel en particulier. La contrainte de ces systèmes est leur niveau de disponibilité exigé. On ne peut pas les traiter après incident comme pour un serveur web par ex car ils constituent le système de contrôle d'un système physique. Le traitement de la phase PRA/PCA [5] est donc particulièrement sensible. Très peu d'entreprises sont aujourd'hui en mesure de traiter cette phase car elles ne disposent pas de la double compétence (processus industriels, sécurité informatique). Les experts sécurité n'ont pas de compétence en SCADA ni en processus industriel. Les experts en SCADA n'ont aucune approche sécurité. De plus, il n'existe pas actuellement en France de formation de niveau bac+5 sur le sujet, qui aborde les deux aspects.

### 3.6 Veille

Il s'agit ici non pas de la veille technologique ou juridique mais d'un métier en tâche de fond qui s'apparente au renseignement, au métier d'analyste défini plus haut. Il s'agit ici d'identifier et de qualifier la menace potentielle. Une entreprise qui travaille dans le domaine nucléaire ou du pétrole par ex. peut identifier l'activisme comme ennemi potentiel pour des raisons idéologiques. Ce qui se traduit par une menace potentielle de type hacktiviste. Ce type de métier peut difficilement se sous-traiter. On est au croisement de l'intelligence économique, de la veille stratégique, de l'expertise technique. Il faut être capable d'identifier les menaces et ensuite les risques au niveau du système.

## 4 Besoins d'enseignement

On peut classer tableau 3 les différents besoins exprimés mais sans affecter de volumétrie précise, trop dépendant du contexte économique. Néanmoins on peut en faire une proposition compte tenu des acteurs qui l'ont exprimée.

| Sujet | Criticité | Volumétrie |
|---|---|---|
| Programmation sécurisée SCADA | *** | *** |
| Sécurité logicielle | ** | *** |
| Sécurité applicative (web) | * | *** |
| Tests d'intrusion | ** | * |
| Aspects fonctionnels | * | * |
| Veille (risques, menaces) | * | * |

TABLE 3 – Typologie des sujets

Il faut préciser que certains sujets ne peuvent être abordés au niveau formation que dans une optique de cyber défense, ce qui exclut toute ouverture à l'international, sauf accord diplomatique spécifique.

5. Plan de Reprise d'Activités / Plan de Continuation d'Activité

# 5 Conclusion

Cette étude a permis de faire la synthèse de l'évolution des métiers, de définir des priorités dans loffre de formation en cyber sécurité. Elle a nécessité de nombreuses contributions. Une telle étude oblige à prendre de nombreux contacts, à se faire comprendre de ses interlocuteurs. Une telle étude doit être conduite par une institution d'enseignement supérieur (université ou école), parce qu'il est d'abord question de formation, mais aussi pour éviter le biais de perception des question, par son caractère désintéressé. Néanmoins, on a pu constater qu'il faut toujours faire comprendre aux entreprises contactées que l'enjeu de questions en apparence indiscrètes ou intrusives est de définir les besoins en enseignement qui à terme relève de leur propre intérêt.