Dossier du Projet Professionnel de l'Étudiant

Secteur d'emploi :

Expert en sécurité informatique – spécialisation : Intelligence artificielle

Hayk ZARIKIAN

Avec Ambre LIS et Solène WEIMAR

Licence 1 – Semestre 2

UFR de Mathématique et d'Informatique

Université de Strasbourg

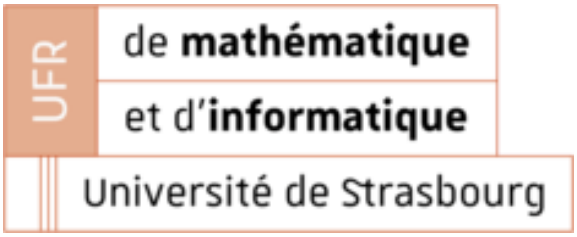


Table des matières

1 Introduction

« Expert en sécurité informatique », pourquoi avoir choisi ce métier ? Après la formation de notre groupe par la similarité de nos passions, nous avons discuté longuement du métier en donnant nos avis et nous avons constaté que nos points de vue et attentes étaient différentes. De plus, notre passion ne se limite pas à la sécurité informatique mais aussi à l'intelligence artificielle, c'est pourquoi nous avons choisi d'étudier le métier d'expert en sécurité informatique avec la spécialisation de l'intelligence artificielle dans le domaine de la sécurité. Personnellement, j'ai pour ambition de devenir expert en sécurité informatique, car je suis passionné par la sécurisation des données personnelles, des réseaux informatiques, des systèmes informatiques de tout genre et je suis contre la cybercriminalité. De plus, le métier est en développement et il connaîtra une expansion dans les années à suivre. Ces raisons ont déterminé le choix de mes études actuelle. Cependant, il reste pour moi comme pour les autres membres du groupe des questions sans réponses. Quelles sont les études à prévoir pour devenir expert en sécurité informatique ? Quelles sont les exigences de ce métier (temps de travail, travail en équipe…) ? Quel impact sur la vie quotidienne ? Quelles compétences doit-on mettre en évidence ? Quelle est l'implication et l'importance de l'intelligence artificielle dans le domaine de la sécurité ? Dans ce dossier, nous aurons les réponses à nos questions et nous en saurons plus sur le métier de l'expert en sécurité informatique. Pour atteindre cet objectif, le groupe a pu obtenir un entretien avec un expert en sécurité informatique via Microsoft Teams qui pourrait répondre à nos questions et à nous éclaircir davantage sur ce métier.

2 Première partie : l'expert en sécurité informatique d'une vision extérieur

2.1 Présentation du métier selon les ressources d'orientation

En quoi consiste le métier d'expert en sécurité informatique ? Quelles sont ses missions, qualités et compétences ? Quelles formations pour devenir expert en sécurité informatique ? Les ressources d'orientation [0][1][2] vont nous aider à répondre à ces questions. L'expert en sécurité informatique ou « hacker éthique » consiste à étudier la sécurité du système d'information d'une entreprise et d'apporter une solution de sûreté (cryptage, pare-feu, antivirus…). Au sein d'une équipe, il joue aussi le rôle d'un chef de projet qui définit des procédures et des règles de sécurité à respecter, et qui assure une veille technologique. Pour ce faire, l'expert détecte toutes les failles de sécurité afin d'anticiper et d'empêcher toute tentative d'intrusion dans le réseau informatique de l'entreprise contre les cybercriminels. L'expert en sécurité informatique doit avoir des connaissances solides en développement système qu'il actualise régulièrement afin d'être à jour concernant les dernières menaces sur internet, doit faire preuve de patience, d'anticipation, doit avoir un respect total de la confidentialité et possède donc une énorme responsabilité envers l'entreprise.

Pour devenir expert en sécurité informatique, il est nécessaire d'effectuer de longues études : un niveau bac+5, diplôme d'ingénieur ou un master dans le domaine de la sécurité informatique et plusieurs années d'expérience, le salaire affiché par les ressources d'orientation est de 2500 à 2900 euros net par mois mais il peut grandement varier selon l'expérience. Ce métier est au cœur de la transformation numérique des entreprises, la sécurité informatique fait partie des métiers les plus recherchés en 2018, il est donc assez simple de trouver un emploi.

2.2 Mon point de vue personnel sur le métier

Pour ma part, je pense que le métier d'expert en sécurité informatique est un métier assez complexe qui exige une connaissance informatique importante (big data, réseaux informatiques, virtualisation et modélisation…) et aussi un état d'esprit persévérant, ambitieux et bien d'autres compétences. Il doit faire preuve d'anticipation et doit toujours être prêt à toute tentative d'intrusion dans le réseau informatique de l'entreprise pour pouvoir contrer l'attaque le plus rapidement possible pour ainsi éviter ou bien limiter les dégâts potentiels. Dans ma vision, l'expert en sécurité informatique est un hacker éthique (activité d'hacking non malveillante) qui pirate pour trouver les failles d'une entreprise pour ensuite la sécuriser. Cependant, je pense qu'il ne doit pas se limiter à la sécurité informatique, il doit être polyvalent et avoir des compétences générales dans l'informatique (programmation, architecture des ordinateurs…) qui serons favorable dans la sécurité.

3 Seconde partie : le métier dans le cadre professionnel

3.1 Le déroulement du métier en entreprise

Grâce l'implication du groupe, nous avons pu obtenir un entretien avec un expert en sécurité informatique via Microsoft Teams qui a pu répondre à nos questions [réponses aux questions]. Qu'est-ce que la vie d'un expert en sécurité informatique ? Un expert en sécurité informatique est un chef de projet au sein d'une équipe ou avec des co-équipiers, le travail en équipe est donc indispensable pour être plus performants [3]. Les horaires sont flexibles et l'expert doit toujours être prêt à intervenir quel que soit le jour et l'heure lors d'une alerte de sécurité. Il faut faire preuve d'une grande autonomie, être responsable et trouver le bon équilibre entre la vie personnelle et professionnelle car la sécurité de l'entreprise dépend de l'expert et de son équipe, pour cela il faut avoir du courage et savoir prendre de la hauteur. Selon l'expérience de l'expert, l'intelligence artificielle est utilisée superficiellement mais son évolution est une nécessité et peut être très utile dans le domaine de la cybersécurité pour la détection d'intrusion et la modélisation des attaques. Globalement, la description du métier par les ressources d'orientation et l'avis du professionnelle sont plutôt équivalente.

3.2 Les points de vue des professionnels sur l'évolution de la sécurité informatique

Nous avons pu récolter plusieurs avis d'expert sur internet et que nous allons faire une synthèse de ce que pense le milieu professionnel sur l'évolution du métier [4][5][6]. La sécurité informatique est de plus en plus présente dans notre société, les perspectives d'évolutions sont sans limites, il y a beaucoup de demande mais peu de profils sorte du lot, il est donc assez simple de trouver un emploi à condition de bien maîtriser certaines compétences et d'être un vrai expert. Il faut prendre son temps, acquérir de l'expérience dans le but d'être polyvalent et devenir une référence dans son domaine, l'auto-formation est un bon facteur d'amélioration. Le directeur général de l'ANSSI [5] (Agence national de la sécurité des systèmes d'information) affirme que la cybercriminalité (données commerciales, espionnage, demande de rançon…) est en hausse car tout ce qui est numérique peut être touché et les objets connectés sont de plus en plus présente dans notre vie quotidienne. Dans les années à suivre, il y aura des attaques de plus en plus visibles, de plus en plus grave. Le sous-directeur de l'ANSSI [6] à récemment parler de la cybersécurité pendant la période sanitaire où la demande de rançon (ransomware ou rançongiciel) est en hausse et que pendant le déconfinement il y a eu une augmentation de la cybercriminalité au sein des entreprises. Globalement, les trois experts prévoient une forte augmentation et une grande gravité de la cybercriminalité dans les années à suivre.

4 Dernière partie : l'intelligence artificielle dans le domaine de la sécurité informatique

4.1 L'intelligence artificielle en général

Voiture autonome, prédiction, détection d'images par catégories, analyser l'environnement, qu'est-ce que l'intelligence artificielle ? L'intelligence artificielle (IA) est l'ensemble des théories et des techniques mises en œuvre en vue de réaliser des machines capables de simuler l'intelligence. L'intelligence artificielle est un processus d'imitation de l'intelligence humaine qui repose sur la création et l'application d'algorithmes exécutés dans un environnement informatique. Depuis cinq ans, l'intelligence artificielle ne cesse d'évoluer et prend de plus en plus de place dans notre vie quotidienne et dans le monde du travail avec la disparition de certains métiers et la création d'autres [7]. Elle est la dernière barrière de l'évolution informatique.

4.2 La sécurisation des systèmes informatiques par l'intelligence artificielle

L'intelligence artificielle est de plus en plus utilisée dans le domaine de la cybersécurité car les cyber-attaques sont de plus en plus nombreuses et complexes, l'IA peut être une solution efficace à ce problème qui pourrait changer la situation dans le monde de la cybercriminalité. Grâce au Machine Learning (apprentissage automatique ou artificielle) qui continue à s'améliorer au fil du temps pour détecter automatiquement les attaques et les virus et ainsi opposer une solide défense aux cybercriminels. L'IA peut aussi être utilisée pour des processus de sécurisation plus performante (authentification plus sécurisés). Les grandes entreprises comme Microsoft et IMB ont chacune un département dédié à la sécurité et à l'IA. Par exemple, la plateforme Windows Defender (anti-virus) est une solution de cybersécurité basée sur l'IA incorporer dans le système d'exploitation Windows [8]. D'après l'expert chargé de notre entretien, « Seul l'IA peut rapprocher les échelles de masse à une gestion centralisée des événements en y apportant un rationnel financier équilibré » [Courbes sur l'impact des cyber-attaques dans les entreprises]. L'intelligence artificielle est donc indispensable dans le domaine de la sécurité informatique qui pourrait changer le monde du travail (financièrement et en sécurisation plus performante du système). Le but est de concevoir via l'intelligence artificielle un programme de sécurisation qui va pouvoir collecter toutes les informations et va pouvoir évaluer s'il y a un risque de sécurité pour le système afin de proposer des remédiations [9].

5 Conclusion

L'expert en sécurité informatique est un métier exigeant qui demande à ce que la motivation, la persévérance et le courage soit au rendez-vous. Il faut être passionné par l'informatique, possédés des compétences dans plusieurs notions (réseau informatique, le big data, cloud computing…) et être prêt à faire de longues études (bac+5). Cependant, il ne suffit pas d'avoir son diplôme pour être expert en sécurité information mais aussi de plusieurs années d'expériences pour être une référence dans le domaine et pour pouvoir ainsi sortir du lot. Ce métier est de plus en plus demandé dans le milieu professionnel car la cybercriminalité ne cesse d'évoluer. La spécialisation de l'intelligence artificielle dans la sécurité informatique est une nécessité car c'est une notion très importante qui peut grandement changer la situation dans le milieu professionnel (financièrement et en sécurisation des systèmes) et à limiter davantage les tentatives d'intrusions. Finalement, l'expert en sécurité informatique est un métier très prometteur et passionnant, cependant il faut s'investir et être motivé pour accumuler des connaissances informatiques importantes. Mon avis sur le métier reste inchangé, le professionnel à confirmer ce que je pensais de l'expert en sécurité informatique et les informations présentes dans les ressources d'orientation.

6 Bibliographie

[0] Onisep, « Expert en sécurité informatique », https://www.onisep.fr/Ressources/Univers-Metier/Metiers/expert-experte-en-securite-informatique

[1] Diplomeo, « Expert en sécurité informatique », https://diplomeo.com/formations-metier-pour-devenir-expert_en_securite_informatique

[2] Jobintree, « Expert en sécurité informatique », https://www.jobintree.com/metier/expert-securite-informatique-765.html#:~:text=De%202500%20%C3%A0%202900%20euros%20brut%20par%20mois

[3] YouTube, « Devenir ingénieur en sécurité informatique », https://www.youtube.com/watch?v=oW5JOOVM6Qg

[4] Systres Consulting, « Avis d'expert : Phillipe Depland », https://www.systresconsulting.com/blog-post/avis-dexpert-philippe-depland-nous-dit-tout-sur-son-metier-de-consultant-en-securite/

[5] YouTube, « Cybersécurité : On aura de plus en plus d'attaques, de plus en plus graves », https://www.youtube.com/watch?v=Qx5Vut1F1mY

[6] YouTube, « François Deruty, Sous-directeur Opérations de l'ANSSI », https://www.youtube.com/watch?v=P63RdltLoL8

[7] YouTube, « Documentaire : Les mystère de L'intelligence Artificielle », https://www.youtube.com/watch?v=9VDUdVxXoWM

[8] Le big data, « Comment l'intelligence artificielle améliore la sécurité », https://www.lebigdata.fr/intelligence-artificielle-securite

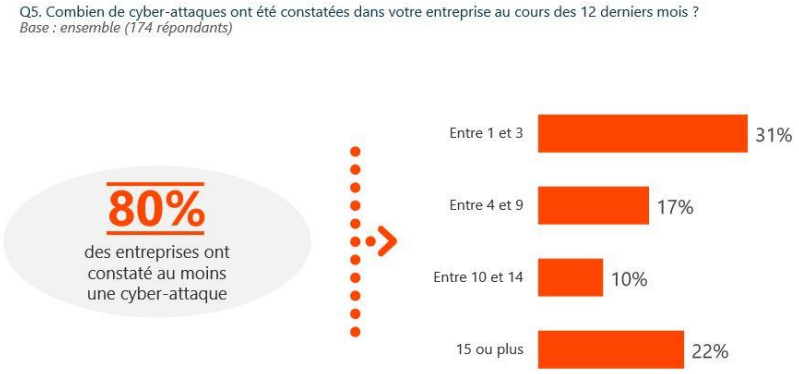
[9] YouTube, « L'intelligence Artificielle au service de la sécurité informatique des entreprises », https://www.youtube.com/watch?v=wotnLs3mvB0

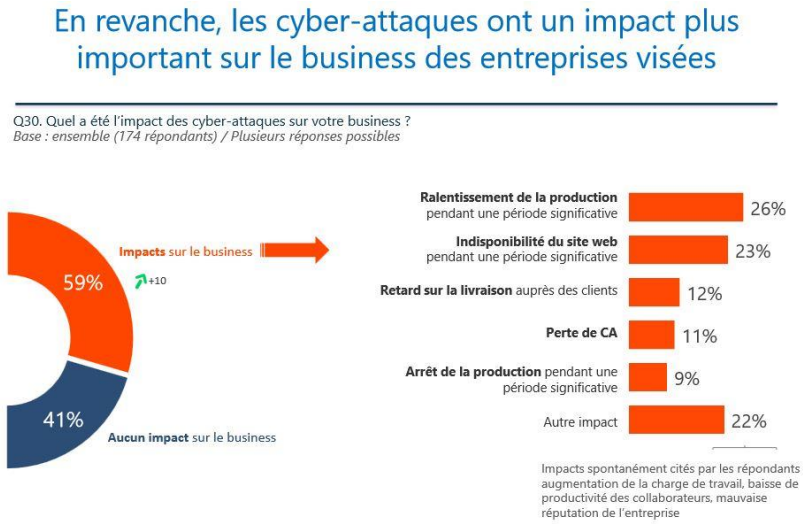
[10] Silkhom, « Cybersécurité : 3 baromètres des cyberattaques à connaître en 2019 », https://www.silkhom.com/cybersecurite-3-barometres-des-cyberattaques-a-connaitre-en-2019/

7 Annexes

7.1 Courbes sur l'impact des cyber-attaques dans les entreprises

Sources : [10]





Description des courbes : 80 % des entreprises ont constaté au moins une cyber-attaque au cours des 12 derniers mois, les conséquences peuvent être le ralentissement de la production, l'indisponibilité du site web, retard sur la livraison, parte de CA, arrêt de la production…

7.2 Questions posées à l'expert en sécurité informatique (avant l'entretien)

Nous avons pu obtenir un entretien par visioconférence avec un expert en sécurité informatique, Pascal MARY de chez Hager Group qui est une entreprise spécialisée dans les installations électriques, basée à Blieskastel, en Allemagne. Nous avons alors pu lui poser les questions ci-dessous : (**en noir : Question**, en vert : réponse)

I/Présentation et domaine d'activité

Quelle est la portée de votre entreprise (locale/nationale/européenne/internationale) ?

Internationale. Le poste de RSSI (Head of Cybersecurity) a été créé en 2019 afin d'adresser et animer la mise en place d'une gouvernance de la cybersécurité pour le groupe Hager. Le périmètre est global et inclut les parties « Informatique de gestion », « usines connectées ou industrie 4.0 » et nos « produits et services connectés (Smart Building, Energy Management et Gestion des intrusions) ».

Comment avez-vous su que vous souhaitiez faire ce métier ?

Je suis passionné par les technologies communicantes. Depuis tout petit, j'étais fasciné par les images animées qui sortent d'un appareil de type téléviseur. J'ai décidé tout petit de savoir comment c'est possible ! la cybersécurité est une continuité, c'est la capacité de comprendre l'attaque pour mieux se protéger.

Quelles études avez-vous faites ?

J'ai fait des études d'électronique à la base (BTS), puis je me suis orienté vers les réseaux et systèmes informatiques (BAC+3), puis j'ai construit mon expérience par la pratique et j'ai eu la chance d'intégrer un cursus MASTER2 en gestion de projets informatiques en alternance à mes 30 ans. A mes 50 ans, j'ai validé mes acquis en Cybersécurité via une formation diplômante dispensée par CentraleSupElec à Paris (via un « executive » certificat). J'ai quelques certifications produites chez IBM, Checkpoint ou Cisco.

Dans quelles entreprises avez-vous travaillé ?

Brasseries Kronenbourg à Obernai / Hager Group à Obernai.

Quelles sont vos responsabilités actuelles ?

Niveau executif Head of Cybersecurity.

Quelle est votre tranche de salaire ?

Joker.

Travaillez-vous en équipe ?

Oui s'il s'agit de travailler au sein d'une équipe ou avec des co-équipiers : collectivement, nous sommes plus performants.

Quel est votre statut chez Hager ?

Cadre dirigeant.

Quels sont vos horaires de travail ?

Flexible.

Quels sont les avantages et inconvénients de votre métier ?

Très grande autonomie, travail en équipe, responsabilités … il faut savoir trouver le bon équilibre entre la vie au travail et la vie personnelle … ça s'apprend avec les difficultés et en sachant s'adapter en gardant sa motivation entière.

Est-ce simple d'allier vie de famille et vie professionnelle ?

Ce n'est pas toujours simple, il faut prendre ses repères et s'y tenir. C'est une question d'auto-discipline … quand on y arrive.

Avez-vous beaucoup d'heures supplémentaires ?

Je ne connais pas d'heures supplémentaires. J'ai une mission à remplir.

Avez-vous des périodes ou des clients pour lesquels la charge de travail est supérieure ?

Les attaquants ou les situations à risque ne se limitent aux heures ouvrées.

II/Sécurité informatique

Quelles qualités sont requises pour travailler dans la sécurité informatique ?

Rester calme, être curieux(se), avoir du courage et savoir prendre de la hauteur.

Comment gérer le travail en équipe sur un domaine aussi sensible ?

Savoir se mettre au niveau des autres, tous domaines et rangs confondus.

Quelles sont les difficultés qui peuvent subvenir lors d'un projet ?

On traite la cybersécurité quand on a fini le projet … C'est très important la sécurité mais là on n'a pas le temps, il faut livrer le client…

Qu'utilisez-vous comme langage de programmation ?

Aucun, les formules Excel suffisent très largement.

Avez-vous des plans d'urgence d'instauré en cas de problèmes (coupure d'électricité, attaque informatique, obsolescence d'un programme…) ?

Oui via des « Play Books ».

III/Intelligence artificielle

Avez-vous recouru à l'intelligence artificielle dans votre travail ?

Oui mais superficiellement.

Que pensez-vous de l'évolution de l'intelligence artificielle dans les métiers de la sécurité informatique ?

C'est une nécessité.

Sa banalisation dans les appareils domestiques (reconnaissance faciale, reconnaissance vocale, cibler les préférences des utilisateurs…) ?

C'est un moyen d'automatiser les tâches mais l'essence de l'IA sont les algorithmes associés. Ils ont bien plus de valeurs que la terminologies IA, surtout dans la cybersécurité.

Est-ce d'après vous une bonne ou une mauvaise chose d'en utiliser sur un domaine aussi sensible ?

La détection d'intrusion et la modélisation des attaques sont des besoins auquel l'IA peut répondre parfaitement. Nous avons de plus en plus d'objets connectés, de plus en plus de menaces avancées et sophistiquées. Seul l'IA peut rapprocher les échelles de masse à une gestion centralisée des événements en y apportant un rationnel financier équilibré.

7.3 Questions posées à l'expert en sécurité informatique (lors de l'entretien)

Dans le cadre de votre métier faites-vous beaucoup de déplacements ?

Non, car Hager Group possède 120 sites à l'internationale, c'est beaucoup trop consommateurs au niveau du temps, on va définir des bonnes pratiques qui sont assimilable par tous les locaux.

En cas d'attaque pendant une heure tardive, êtes-vous dans l'obligation d'être disponible et répondre aux besoins ?

Hager Group offre un support 24/7, il y a une équipe opérationnelle qui sont formées, leur mission est d'assurer la continuité du service. En cas d'immobilisation d'une usine, les techniciens doivent intervenir dans un délai maximum de 45 minutes. L'entreprise a mise en place des « Play Books (guide) » qui consiste à agir de la bonne manière en cas de cyber-attaque.

Est-ce que le métier consiste seulement à la sécurisation des systèmes ou bien aussi à une sécurité offensive ?

On va surtout avoir une approche de défense mais par contre on apprend l'attaque pour mieux se défendre. On fait très régulièrement des tests offensifs, on va faire des tests éthiques via des « hackers éthique », ce sont des sociétés spécialisées qui vont tester nos systèmes pour que nous, on puisse juger les vulnérabilités.

Quelles sont les types de personnes qui tente de s'introduire dans le système en général (particulier, la concurrence…) ?

Ce sont souvent des individus qui font des tentatives d'intrusions avec un niveau d'étudiant par contre on a constaté depuis la crise sanitaire que ces attaques sont de plus en plus organisées par des organisations frauduleuses. Tous les jours, nous avons des scans de port, des alertes (injection de code).

Est-ce qu'avez-vous recours à Hackathon, nuit de l'info ou à ce type d'événements pour mettre votre sécurité à l'épreuve ?

Non, pas pour les aspects de cybersécurité, on participe aux Hackathon mais plutôt sur des initiatives qui touche l'innovation. On ne souhaite pas nécessairement exposer notre niveau de sécurité, on préfère être maître de notre sécurité via des processus que nous avons déterminés.

Avez-vous eux des cas d'attaques automatisées qui pourrait potentiellement ressembler à de l'intelligence artificielle ?

Oui, j'en ai moins la preuve mais une certitude, l'intelligence artificielle pour mener une attaque, elle a surtout un rôle de découverte et d'énumération des données présente sur internet notamment sur le Dark Net et aujourd'hui on trouve des outils même commerciaux pour faire des découvertes, je pourrais mettre le mot-clé Hager et le système va faire une énumération des données concernant le mot Hager ou qui s'y rattache. L'intelligence artificielle n'est pas là pour mener une attaque mais découvrir ce qu'on a, ce que la cible a.

Avez-vous un outil qui faciliterais la détection d'intrusion ?

Nous avons des outils en place qui permette de détecter le minimum des choses, nous avons des outils de surveillance des sites Web qui va vérifier que les niveaux de sécurités (sécurisation/expirations des certificats, adresse email publiée sur le Dark Web…).

Ne pensez-vous pas que la course entre la cybercriminalité et cybersécurité devienne obsolète pour l'humain et qu'il vaudrait se reposer sur l'intelligence artificielle pour y apporter un changement concret ?

Oui et non, oui parce que la masse d'information assimiler par l'humain est faible par rapport à un système d'intelligence artificielle qui pourrait collecter ces informations plus rapidement et en quantités mais de l'autre côté l'intelligence artificielle est basée sur des algorithmes que l'humain a faits et on fera toujours dire à la machine ce que l'humain a bien voulu lui faire exécutée.