



Présentation Métier Analyste Sécurité 21/10/2021

Almamy Touré
Doctorant CIFRE

IBM Client Innovation Center
France



Présentation du domaine métier

"La cybersécurité ? "

"Qui n'a jamais entendu parler de cyberattaques ?"

Le domaine "cybersécurité" est au coeur de tous les débats, vu les cyberattaques constantes, les risques et impacts associés (**192 attaques** enregistrées en **France 2020 avec une rançon de 130k** en moyenne, selon l'**ANSSI** avec une hausse de 255% vs 2019).

La supervision de la sécurité revient sur le devant de la scène en raison des nouvelles réglementations auxquelles certains domaines d'activités sont soumis.

Les Systèmes d'Information (SI) deviennent de plus en plus complexes d'année en année, donc tout type d'entreprise comme les banques, les opérateurs de téléphonie, les assurances, services publics, les OIV ... fait appel à ce profil métier.

Le profil métier est très recherché et bien rémunéré car il y'a un manque d'experts dans le domaine.

Concept : "Il est plus facile d'attaquer que de défendre un SI."

La question n'est plus: "Est-ce que mon SI peut se faire attaquer ?" mais "Quand sera t il attaqué ?"



Formation initiale

2021 – Aujourd'hui : Doctorat\Thèse CIFRE IBM–LAMIH

2017 – 2019 : Master IRCOMS labellisé ANSSI-17-003 – UPHF

2016 – 2017 : Licence Professionnelle Réseaux et Télécommunications - UPHF

2014 – 2016 : DUT Réseaux et Systèmes Informatiques

- **Métier de passion qui nécessite des bases de formation**
- **Initiation aux outils, méthodes, techniques : curiosité**



Parcours professionnel

02/2021 - Aujourd'hui : Threat Expert / CIFRE PhD Student

12/2019 - 02/2021 : Threat Analyst

09/2017 - 09/2019 : Ingénieur Cybersécurité en alternance

04/2017 - 09/2017 : Superviseur Réseaux



Privilégier beaucoup les expériences professionnelles : stages, alternance, contact avec les professionnels, les retours d'expériences



Rôles et fonctions dans le métier

- Garantir la sécurité d'un système d'information (SI)
- Assurer la surveillance , la détection et l'analyse d'incidents de sécurité en 24/7
- Gérer la coordination, le suivi et le reporting des incidents de sécurité
- Prendre en charge des alertes remontées par les bonnes équipes
- Proposer un plan d'investigations et de recommandations adapté
- Proposer et implémenter les cas d'usages (scénarios d'attaque)
- Effectuer du hunting et de la veille technologique
- Apporter une expertise technique sur les différents sujets (Réseaux, Systèmes, Sécurité) en fonction de l'environnement



Aptitudes techniques et comportementales pour le poste

Aptitudes techniques :

- Connaissances en informatique
 - Réseau (Adressage, Routage, protocoles, ...)
 - Système (Windows, Linux)
 - Scripting (Bash, Python, ...)
 - Sécurité (Firewalling, OWASP, CVE,)
- Maîtrise des techniques d'intrusion, cyberattaques et de corruption des SI
- Connaissance des règles de sécurité des SI
- Qualité rédactionnelle

Aptitudes Comportementales :

- Travail en équipe
- Autonomie et organisation
- Capacité d'analyse et de synthèse
- Force de proposition
- Rigueur, méthodologie de travail
- Communication et expression orale



Vision du métier étudiant/vie professionnelle

- L'école nous apprend les bases, les méthodologies qu'il faut savoir appliquer en fonction du contexte, et du besoin.
- Le monde professionnel est plus complexe que le monde académique :
 - soyez ouverts d'esprit
 - soyez passionnés
- Dans le monde professionnel, vous serez beaucoup sollicités :
 - Formez-vous
 - Saisissez les opportunités
 - Croyez en vous et fixez-vous des objectifs à court et long termes
 - Ayez un équilibre de vie (professionnel vs personnel)

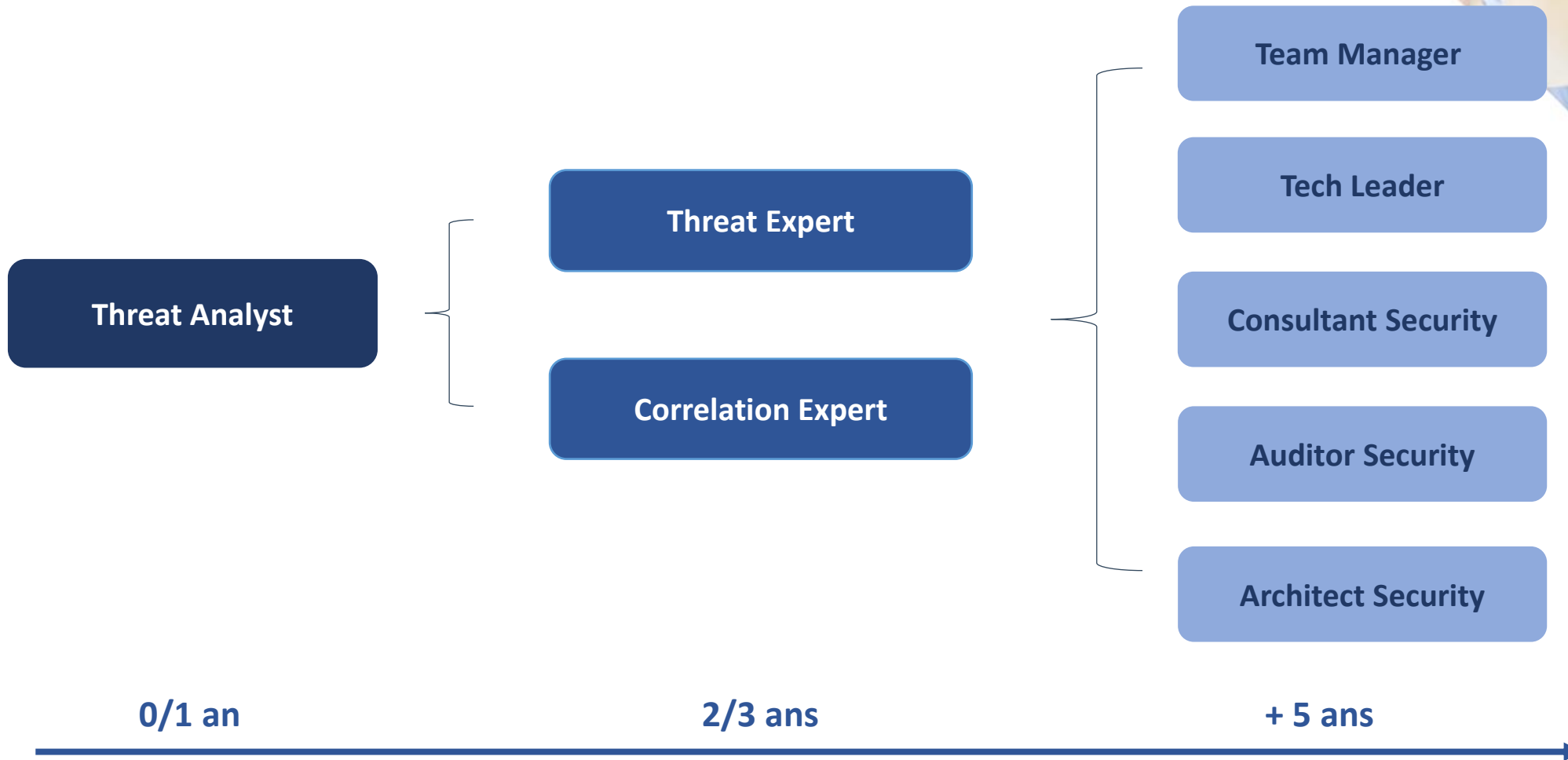


Qu'apporte le métier?

- Se responsabiliser, et avoir de la conscience professionnelle
- Une ouverture d'esprit, une autre façon de voir les choses, vu les différentes tactiques et techniques d'attaque
- "Repousser une cyberattaque" apporte un sentiment de satisfaction personnelle
- Le dépassement de soi-même car le métier nécessite un développement continu des compétences
- Être un couteau suisse dans le domaine informatique



Quelles sont les perspectives d'évolution du métier



A group of four people are gathered around a wooden table in a bright, modern setting, possibly a cafe or office. They are all looking at their mobile devices. A man in a light blue shirt is on the left, holding a tablet. A woman with long dark hair is next to him, also looking at a device. In the foreground, a man in a bright blue polo shirt is pointing at a smartphone held by a woman with blonde hair. A white coffee cup is on the table. The background is blurred, showing more of the interior space.

Questions/ Réponses