



# Présentation Métier **Analyste Sécurité** 20/10/2022

---

Ali BELHAJ

ThreatOps Manager

**IBM Client Innovation Center**  
France



# Présentation du domaine métier

## "La cybersécurité ? "

"Quelle est la première ou dernière cyberattaque dont vous avez entendu parler ?"

### Chiffres opérationnels clés

2 089 signalements	1 057 incidents	8 incidents majeurs	17 opérations de cyberdéfense
--------------------	-----------------	---------------------	-------------------------------

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 tous types d'entreprise comme les banques, les opérateurs de téléphonie, les assurances, services publics, les OIV ... font appel à ce profil métier.

C'est un des métiers identifié "sous tension" par le gouvernement Français : il est très recherché et il y a peu de candidats qualifiés.

**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

---

**2014 – 2016 : Master professionnel en Cyber-sécurité**

**2007 – 2010 : Licence Professionnelle Réseaux et Télécommunications**





# PARCOURS PROFESSIONNEL

2022- Aujourd'hui : ThreatOps Manager

2019 – 2022 : SOC Team Leader

2016 – 2019 : Consultant en Cybersécurité

2014 – 2016 : Master professionnel en Cyber-sécurité

2012 – 2014 : Analyste en Cybersécurité

2010 – 2014 : Administrateur Système et réseaux

 IBM Security

 i-TRACING  
CYBERSÉCURITÉ

digital.security

SAT2I

Bell

GOAL →



# 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 la notification des incidents de sécurité
- Prendre en charge des alertes remontées par les équipes appropriées
- Proposer un plan d'investigations et de recommandations adapté
- Proposer et implémenter les cas d'usages de cybersécurité (scénarios d'attaque)
- Effectuer du « hunting » de compromission 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, Regex ...)
  - Sécurité (Firewalling, OWASP, CVE, ....)
- **Maîtrise des techniques d'intrusion, cyberattaques et de corruption des SI**
- **Connaissances des politiques de sécurité des SI**
- **Qualité rédactionnelle**

## Aptitudes comportementales

- **Travail en équipe**
- **Autonomie et organisation**
- **Capacités 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?

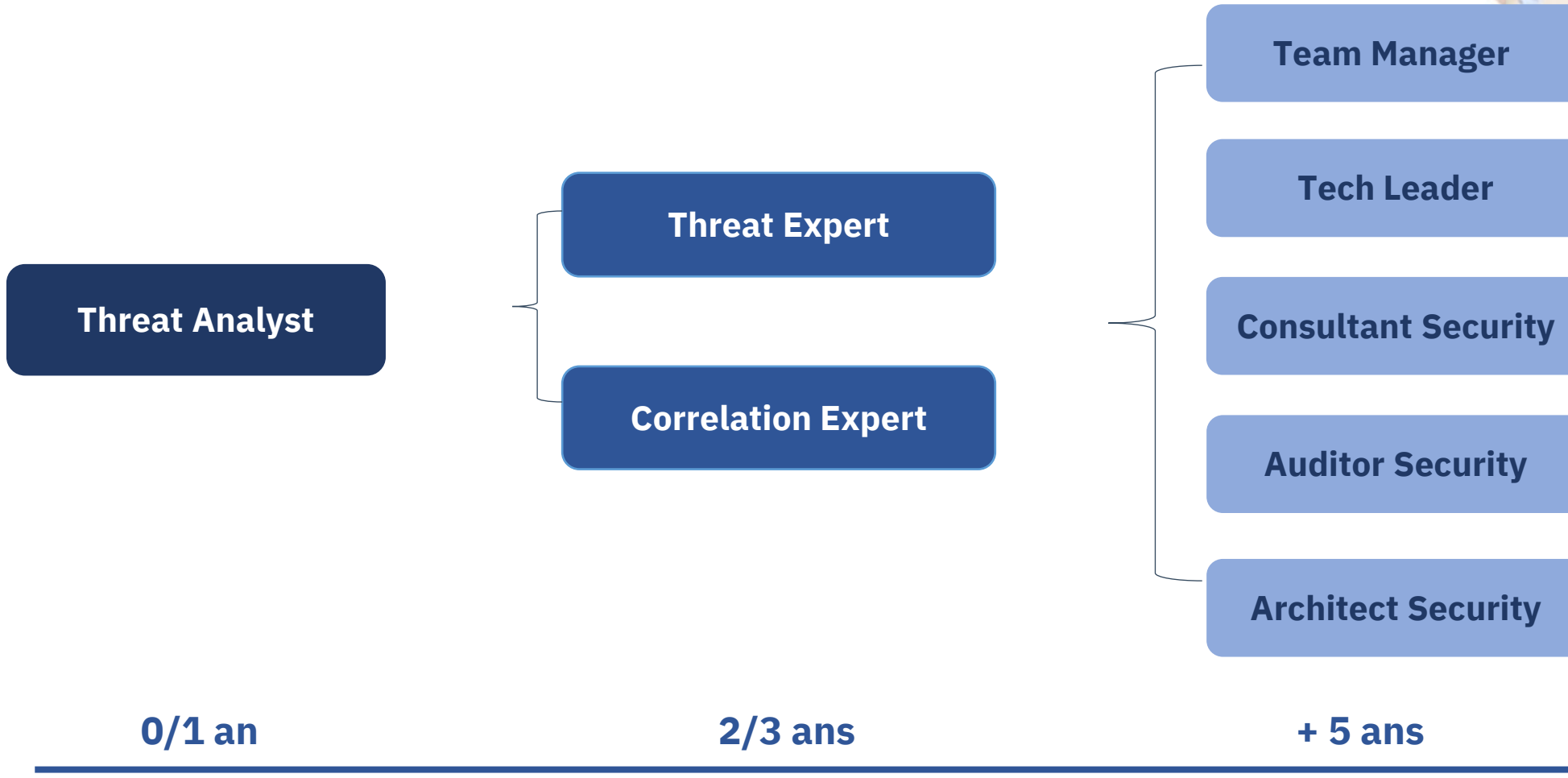
---

- 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'attaques
- "Eviter ou 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



# Autres profils dans le domaine «cybersécurité»

**Admin Infrastructure sécurité**

**Intégrateur de solutions**

**Pentester**

**Auditeur - Gouvernance**

**Ingénieur IAM**

**Ingénieur Sécurité  
Opérationnelle**







*Questions/ Réponses*