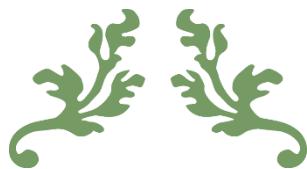


THEIVENDRAM HariHarani, 1R3



---

# **RAPPORT PFMP N°1**

---

22 Novembre au 17 Décembre (soit 20 jours)



## **BNP PARIBAS**

BACCALAUREAT PROFESSIONNEL SYSTEMES NUMERIQUES

Lycée Professionnel Gustave Ferrié,  
7 Rue des Ecluses St Martin, 75010 Paris  
01 42 02 19 55

# SOMMAIRE

I. REMERCIEMENTS .....	3
II. INTRODUCTION .....	4
III. PRESENTATION DE L'ENTREPRISE .....	5
a. Coordonnées .....	5
b. Situation géographique .....	5
c. Histoire de BNP Paribas dans la dimension économique .....	5
d. Organigramme de l'entreprise .....	7
e. Organigramme du groupe CYBER SOC .....	9
IV. COMPTE-RENDU D'ACTIVITES .....	10
V. ETUDE DE CAS .....	11
a. CCTP .....	11
b. INTRODUCTION .....	11
Qu'est-ce que la threat intelligence ? .....	11
Qu'est-ce que le renseignement sur les menaces ? .....	12
Pourquoi les renseignements sur les menaces sont-ils importants ? .....	12
Quel est le cycle de vie des renseignements sur les menaces ? .....	13
c. Évolution du logiciel Emotet .....	15
Qu'est-ce qu'Emotet ? .....	15
Le nom Emotet .....	15
Qui Emotet cible-t-il ? .....	16
Quels sont les appareils exposés à Emotet ? .....	16
Comment se propage-t-il ? .....	16
Un programme malveillant particulièrement destructeur .....	16
L'infrastructure du programme malveillant réduite à néant .....	17
Le retour d'Emotet en Novembre 2021 .....	18
VI. SYNTHESE .....	20
VII. ANNEXES .....	21
VIII. CONSEILS .....	24
a. Sites actualités cyber .....	24
b. Ecole .....	24

# I. REMERCIEMENTS

Il m'est agréable à remercier M. Cyril RIGHI, manager de l'équipe Cyber Security Operation Center (SOC) de BNP Paribas, pour m'avoir donnée l'opportunité de réaliser ce stage.

D'autre part, je remercie plus particulièrement M. Aurélien CIRACQ et Mme. Patria AZZAM, mes tuteurs qui ont tenu le rôle de guide durant cette insertion professionnelle. Ils ont su me rassurer et me donner les moyens de concrétiser des projets en autonomie, ainsi qu'en équipe à leurs côtés. Merci à l'équipe Cyber SOC pour son soutien et son écoute, chacun a su rendre mon stage plus agréable et instructif.

Je remercie par ailleurs tous mes enseignants pour toutes les connaissances qu'ils m'ont inculquées. Je souhaite que le travail réalisé soit à la hauteur de leurs espérances.

## II. INTRODUCTION

Du 22 novembre au 17 décembre 2021, j'ai effectué un stage au sein de l'entreprise BNP Paribas, située à Montreuil. Au cours de ce stage que j'ai réalisé dans le département du Cyber Security Operation Center (SOC), j'ai pu m'intéresser à la cybersécurité.

Plus largement, ce stage a été l'opportunité pour moi de comprendre mieux le monde de la cybersécurité. Mes maîtres de stage étant dans la threat intelligence, j'ai pu apprendre dans d'excellentes conditions.

L'élaboration de ce rapport a pour principale source, les différents enseignements tirés des tâches auxquelles j'étais affectées. Enfin, les nombreux entretiens que j'ai pu avoir avec les employés des différents services de la banque m'ont permis de donner une cohérence à ce rapport.

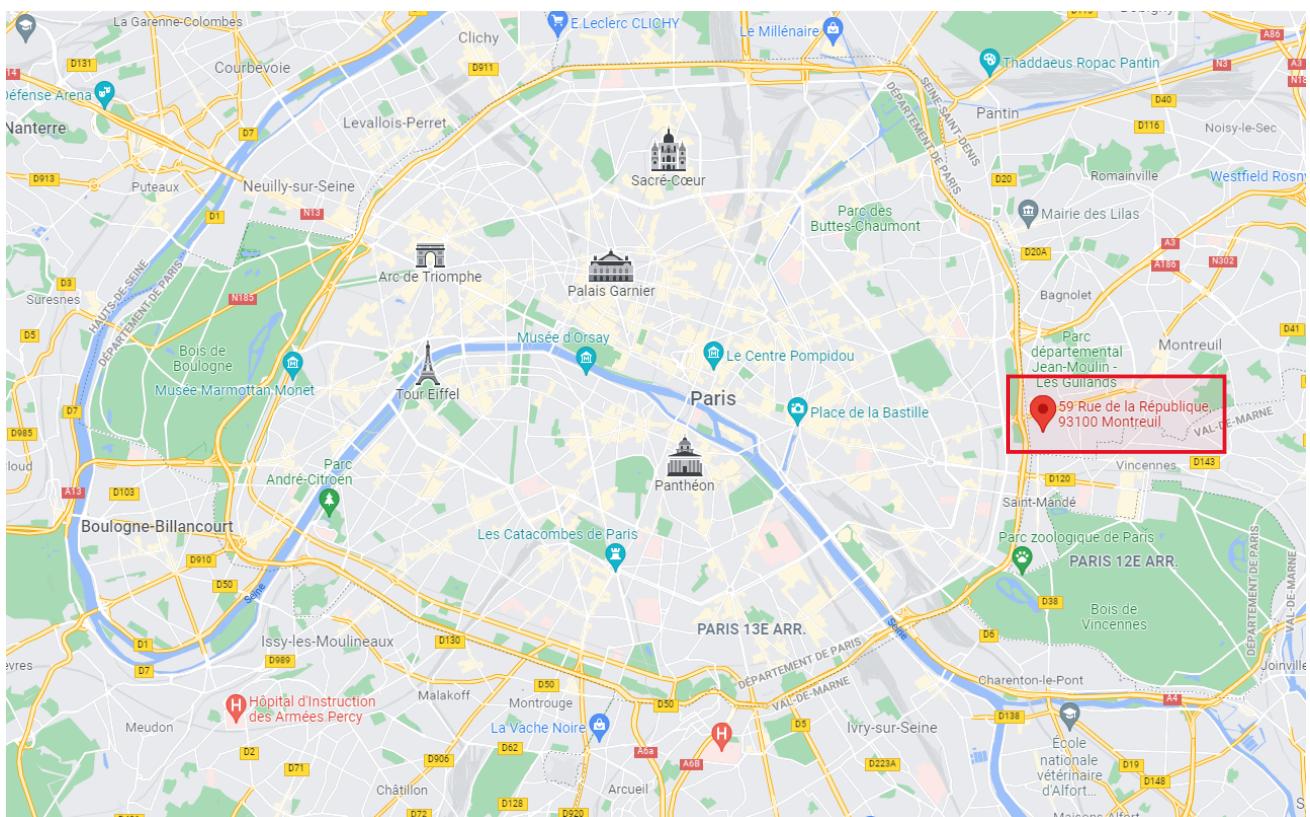
En vue de rendre compte de manière fidèle et analytique de la période passé au sein de BNP Paribas, il paraît logique de présenter à titre préalable l'environnement informatique du stage, à voir le secteur de la cybersécurité. Enfin, il sera précisé les différentes missions et tâches que j'ai pu effectuer au sein du département, et les nombreux apports que j'ai pu en tirer.

# III. PRÉSENTATION DE L'ENTREPRISE

## a. Coordonnées

Nom : BNP Paribas – Valmy 1  
Adresse : 59 Rue de la République, 93100 Montreuil  
N° de téléphone : 06 33 30 36 66  
N° de Siret : 662 042 449 000 14

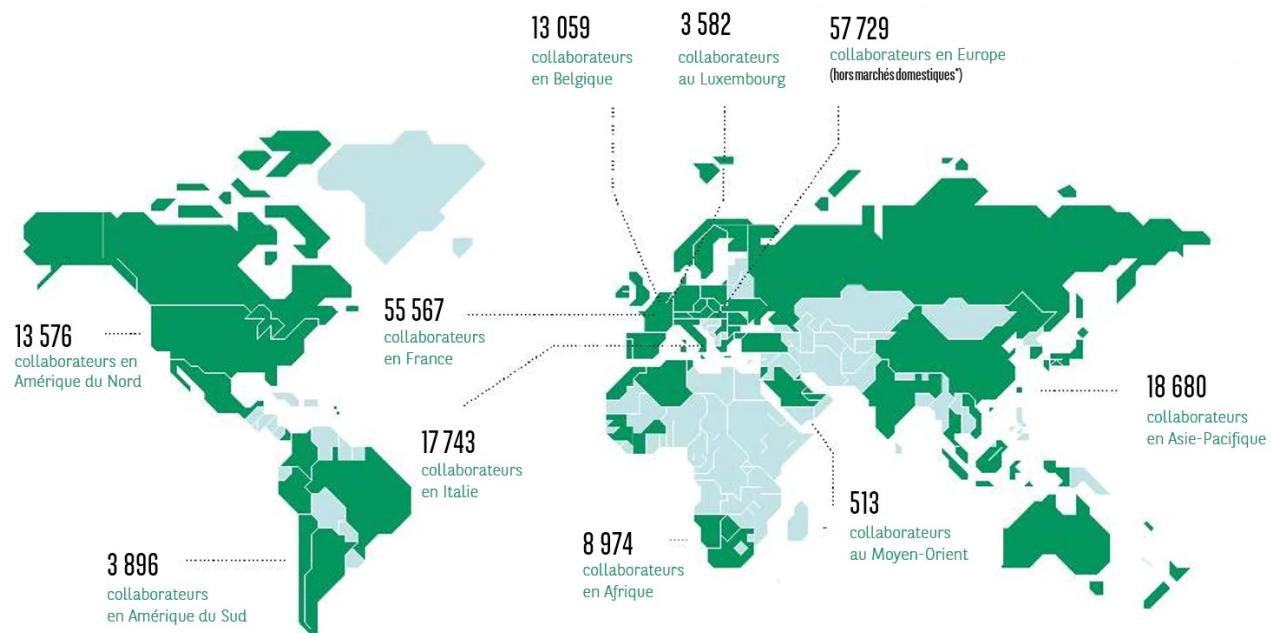
## b. Situation géographique



## c. Histoire de BNP Paribas dans la dimension économique

L'histoire de BNP Paribas débute au XIXème siècle, alors que les banques ancêtres du Groupe naissent et se développent. Entraînées par le formidable essor industriel de l'Europe, elles drainent l'épargne nécessaire au financement du développement économique. En remontant aux sources du Groupe, ce sont près de 2 siècles d'histoire du secteur de la banque, mais aussi d'histoire de l'Europe, voire du monde, que l'on peut parcourir.

BNP Paribas est présent dans 68 pays avec plus de 193 000 collaborateurs dont près de 148 000 en Europe. Le Groupe accompagne tous ses clients – particuliers, associations, entrepreneurs, PME-ETI, grandes entreprises et institutionnels – dans la réussite de leurs projets grâce à ses solutions de financement, d'investissement, d'épargne et de protection.



## Quelques chiffres d'affaires en 2020 :

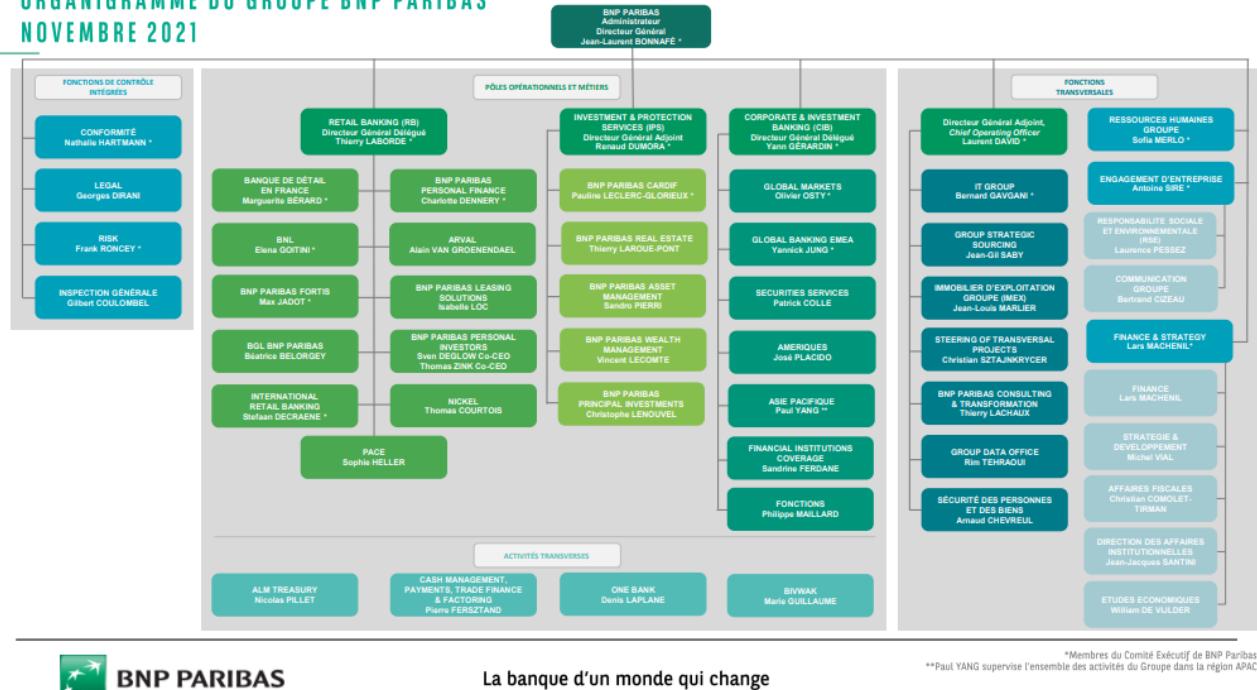
- 44,3 Md€ Produit net bancaire
- 7,1 Md€ Résultat net part du groupe
- 432 Md€ Réserve de liquidité immédiatement disponible
- 809 Md€ de crédits à la clientèle
- 1 165 Md€ d'actifs gérés par les équipes de l'Asset Management de BNP
- 396 Md€ de financement levé pour les clients sur les marchés de crédits syndiqués, d'obligation et d'actions
- N°1 Mondial avec 24,2 Md€ d'obligations durables à fin 2020

## Dates importantes :

- 1822 : création à Bruxelles de la Société générale de Belgique
- 1848 : création du Comptoir National d'Escompte de Paris (CNEP) et Comptoir National d'Escompte de Mulhouse
- 1872 : création de la Banque de Paris et des Pays-Bas (Paribas)
- ...
- 1966 : fusion du CNEP et de la BNCI pour former la banque Nationale de Paris (BNP)
- 1993 : privatisation de la BNP

## d. Organigramme de l'entreprise

### ORGANIGRAMME DU GROUPE BNP PARIBAS NOVEMBRE 2021



La banque d'un monde qui change

\*Membres du Comité Exécutif de BNP Paribas.

\*\*Paul YANG supervise l'ensemble des activités du Groupe dans la région APAC.

Dans cet organigramme, on y trouve tous les membres du comité exécutif de BNP Paribas. BNPP est une organisation très complexe. On peut voir aussi les différentes filiales de cette entreprise.

### Filiale :

Chez BNPP, il y a 3 pôles opérationnels :

#### 1. Domestic Markets (DM) qui regroupe :

4 banques de détails dans la zone euros :

- BDDF en France
- Fortis en Belgique
- BNL en Italie
- BGL au Luxembourg

4 métiers spécialisés :

- Arval : spécialisé dans la location de voiture
- Leasing : offre des solutions locatives et du financement
- PI (Personal Investor) : propose des solutions d'épargne et du courtage en ligne
- Nickel : présente des services bancaires alternatif

## 2. International Financial Services (IFS) qui regroupe :

2 activités :

- PF (Personal Finance) : qui propose aux clients des solutions de crédit
- Cardif : qui propose des solutions d'épargne et de protection

4 métiers leaders de la gestion institutionnelle et privée :

- Wealth Management : banque privée de référence mondiale
- Asset Management : spécialiste de la gestion d'actifs
- Real Estate : s'occupe des services immobiliers
- Les banques de détails hors zone euro :
  - TEB en Turquie
  - BoW aux USA
  - Etc.

## 3. Corporate Investment Banking (CIB) qui offre des solutions sur mesure :

- Corporate Banking : dans les domaines des financements, de la gestion de trésorerie et du conseil financier aux entreprises
- Global Markets : dans le domaine des marchés de capitaux
- Securities Services : dans les services de conservation et d'administration de titres

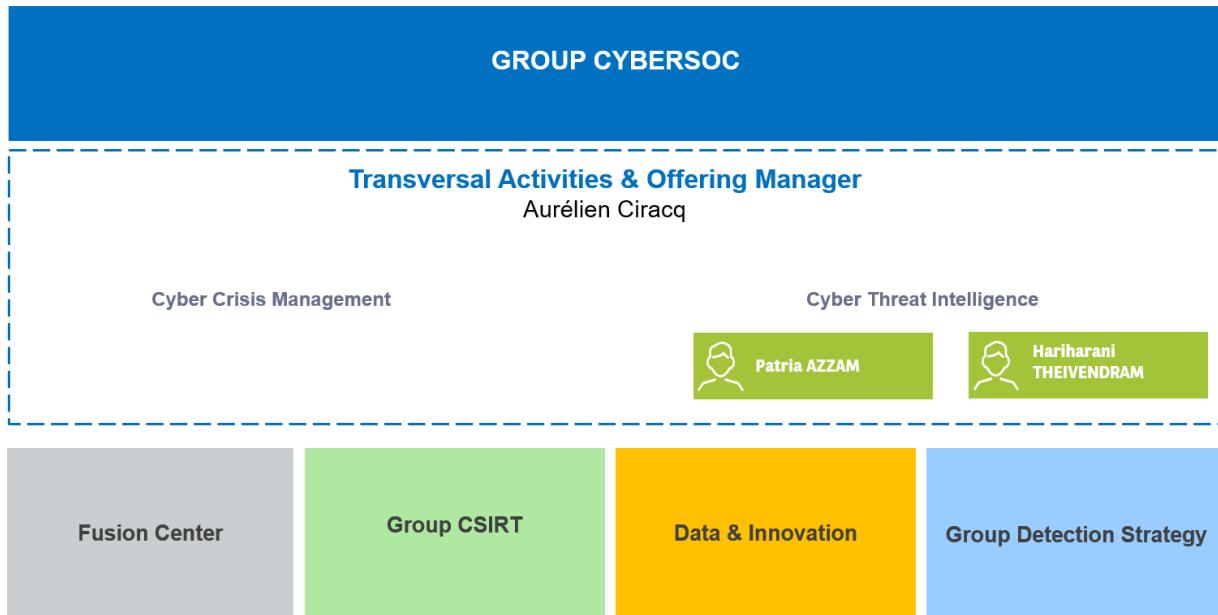
**Partenaires (exemple de partenaires) :**

- Handisport
- Festival Cinéma
- Roland Garros
- Etc.

**Concurrents (la liste n'est pas exhaustive) :**

- Société Générale
- Crédit Agricole
- Crédit Mutuel
- Etc.

## e. Organigramme du groupe CYBER SOC



Lors de mon stage, j'ai travaillé avec le groupe CYBER SOC. Voici les rôles des différentes activités du département :

- **Fusion center**: gère la gouvernance et gestion des risques de cyber-fraud (la fraude est une attaque commise dans l'intention de voler de l'argent à des clients ou à l'entreprise).
- **CSIRT (Computer Security Incident Response Team)**: s'occupe de faire la réponse aux incidents de sécurité cyber.
- **Data & Innovation**: pilote la collecte, la transformation et l'enrichissement des données dans le but d'augmenter les capacités d'investigation et de détection ainsi que d'automatiser tous les processus de pré et post détection.
- **Detection Strategy**: gère la gouvernance du programme Cyber SOC afin d'améliorer les capacités de détection du Groupe.
- **Transversal Activities & Offering Management**: définit et maintient la feuille de route des différents services du SOC. Cette activité inclut en plus :
  - **Cyber Threat Intelligence**: collecte d'information sur les incidents de cybersécurité qui ont touché d'autres entreprises pour améliorer la capacité de détection du Groupe.
  - **Cyber crisis management**: préparation d'un exercice d'entraînement, pour tester la procédure déjà définie afin d'être prêt lors d'une vraie attaque.

## IV. COMPTE-RENDU D'ACTIVITES

Pendant mon stage, j'ai pu participer à divers :

**Rencontres avec :**

- Les membres de l'équipe SOC m'ont expliqué leurs rôles.
- Les Pentesters (penetration test) : qui m'ont permis de voir comment ils faisaient leurs tests d'intrusions c'est-à-dire, simuler une attaque d'un utilisateur mal intentionné, pour évaluer la sécurité d'un système d'information.

**Réunions :**

J'ai participé à des réunions en Visio-conférences sur les thématiques suivantes :

- **Purple Team** : Cette équipe a le rôle d'interfacer avec la « blue team » (défenseur) et la « red team » (testeur) afin d'améliorer la défense du système d'information (SI).
- **Phishing** : Ce type d'attaque permet au fraudeur de se faire passer pour un organisme connu (exemple-une banque) pour tromper la victime. Ainsi, il va envoyer un mail, avec un lien vers des sites web infectés, pour voler les coordonnées bancaires de la cible.
- **Cyber Crisis exercice**

**Formations :**

J'ai participé aux formations ci-dessous qui sont obligatoire pour tous les employés :

- **Sensibilisation sur la cybersécurité**
- **Sécurisation des bureaux :**

Le badge d'un collaborateur chez BNPP est très important car c'est son passeport et il doit l'avoir toujours sur soi. Ce badge couvre plusieurs niveaux de sécurité :

- Les accès physiques : pouvoir badger à l'entrée du bâtiment, la circulation entre les étages et pour le Groupe SOC, l'accès à l'espace sécurisés aux personnes qui y travaillent.
- Les accès logiques : utiliser pour la connexion du poste professionnelle et authentification sur les applications de travail par le certificat présent sur la carte à puce. Lorsque l'on quitte le bureau, il faut toujours :
  1. Verrouiller les fenêtres
  2. Fermer la session de l'ordinateur
  3. Ranger les documents dans les placards et les fermer à clefs.
  4. Détruire les documents à jeter.

**Activités personnelles :**

Veille média (Média Watch en anglais) : lecture des actualités mondiales pour suivre les dernières menaces, vulnérabilités et attaques cyber.

# V. ETUDE DE CAS

## a. CCTP

- **Contexte** : dans le cadre de la Cyber Threat Intelligence, nous souhaitons étudier le retour du logiciel malveillant « Emotet » qui cible le secteur financier et représente une menace pour BNP Paribas et ses clients.
- **Objectifs à atteindre** :
  - Expliquer ce que la Cyber Threat Intelligence (son but, son cycle de vie et les différents niveaux)
  - Décrire l'histoire du malware « Emotet » qui a été démantelé par les autorités Ukrainiennes en Janvier 2021 et se concentrer sur son retour en Nov. 2021.
- **Périmètre** : Donner une vision stratégique d'une menace concrète qui pèse sur le secteur financier en abordant les risques internes (collaborateurs) et externes (clients).
- **Description fonctionnelle du besoin** : rédiger un document avec un schéma qui résume l'histoire de la reprise d'activité du malware « Emotet ».

## b. INTRODUCTION

### → Qu'est-ce que la threat intelligence ?

La connaissance est toujours l'élément de base de la construction d'une défense contre les cyberattaques. Après tout, les entreprises qui comprennent les vulnérabilités<sup>1</sup> et les TTP<sup>2</sup> (Tactics, Techniques & Procedures) des attaquants peuvent se préparer à l'avance contre les attaques. C'est ainsi qu'émerge la Threat Intelligence, un outil de prévention des attaques informatiques.

De nos jours, les cyberattaques contre les administrations et les entreprises sont de plus en plus fréquentes. Les attaquants recherchent généralement des données confidentielles pour causer des dommages ou attaquer des cibles plus importantes.

Après avoir identifié ces problèmes, les concepteurs ont conçus ce qu'on appelle les renseignements sur la CTI (Cyber Threat Intelligence). C'est une discipline axée sur la technologie du renseignement, dans le but de collecter et d'organiser les informations liées aux cyberattaques et aux menaces. Aujourd'hui, 78% des entreprises qui ont utilisé cette règle ont constaté leur capacité à répondre aux attaques.

---

<sup>1</sup> Une faille de sécurité, qui provient dans la majorité des cas d'une faiblesse dans la conception d'un système d'information (SI), d'un composant matériel ou logiciel.

<sup>2</sup> Décrit comment les threat actors orchestrent, exécutent et gèrent leurs attaques.

À l'aide de la CTI, les organisations peuvent se défendre contre les états de menace et les scénarios d'attaque. En tant que système d'alerte précoce, la discipline fournit des données collectées pour la conception d'armes contre des attaques potentielles.

La CTI s'est mobilisé tant sur le plan technique que stratégique. Cette dernière est la mieux adaptée pour transformer l'information en véritables mesures défensives. Si nous utilisons la discipline de manière pratique, elle complétera la cybersécurité en tant qu'élément préventif.

## → Qu'est-ce que le renseignement sur les menaces ?

Les renseignements sur les menaces, également appelés les renseignements cybermenaces, sont des informations recueillies auprès de diverses sources sur les attaques actuelles ou potentielles contre une organisation. Les informations sont analysées, affinées et organisées, puis utilisées pour minimiser et atténuer les risques de cybersécurité.

L'objectif principal du renseignement sur les menaces est de montrer aux organisations les différents risques auxquelles elles sont confrontées face aux menaces externes, telles que jour zéro menaces<sup>1</sup> et menaces APT (Advanced Persistent Threat)<sup>2</sup>. Les renseignements sur les menaces comprennent des informations et un contexte détaillé sur des menaces spécifiques, telles que les threat actors<sup>3</sup> attaquent, leurs capacités et leur motivation, et les IoC (Indicator of Compromise)<sup>4</sup>. Grâce à ces informations, les organisations peuvent prendre des décisions éclairées sur la façon de se défendre contre les attaques les plus dommageable.

## → Pourquoi les renseignements sur les menaces sont-ils importants ?

Le renseignement sur les menaces fait partie d'un plus grand renseignement de sécurité stratégique. Il comprend des informations relatives externes et internes, ainsi que le processus, politiques et outils utilisés pour collecter et analyser ces informations. Bon nombre de ces ajustements peuvent être automatisés afin que la sécurité reste alignée sur les dernières informations en temps réel.

Il existe quatre types de renseignements sur les menaces : stratégiques, tactique, technique et opérationnel. Ces quatre éléments sont essentiels pour établir une évaluation complète des menaces.

---

1 « Zero-day » (ang.) désigne une faille de sécurité informatique qui n'est pas encore connue ou corrigée par l'éditeur du produit concernée.

2 Menaces persistantes avancées (APT) sont des opérations à long termes conçus pour infiltrer et/ou exfiltrer le plus de données de valeur possibles sans être découvert.

3 Une personne ou un groupe de personne malveillant qui participe à une action destinée.

4 Un artefact observe sur un réseau ou dans un système d'exploitation qui indique, avec un haut niveau de certitude, une intrusion informatique.

- **Veille stratégique sur les menaces**

*« L'observation et l'analyse de l'environnement scientifique, technique, technologique et économique de l'entreprise pour en détecter les menaces et saisir les opportunités de développement ».*

Cette analyse résume les cyberattaques potentielles et les conséquences possibles pour les publics et les parties prenantes non techniques, et aussi les décideurs. Il est présenté sous forme de livres blancs, des rapports et de présentations, et est basé sur une analyse détaillée des risques et tendances émergents du monde entier. Il est utilisé pour brosser un aperçu du haut niveau du paysage des menaces d'une industrie ou d'une organisation.

- **Renseignements tactiques sur les menaces**

Le renseignement tactique fournit des informations sur les TTP utilisées par les acteurs de la menace. Il est destiné aux personnes directement impliquées dans la protection des ressources informatiques et de données. Il fournit des détails sur la manière dont une organisation peut être attaquée en fonction des dernières méthodes utilisées et des meilleurs moyens de se défendre ou d'atténuer les attaques.

- **Renseignements techniques sur les menaces**

Ces informations se concentrent sur les signes qui indiquent qu'une attaque commence. Ces signes comprennent la reconnaissance, l'armement et la livraison, tels que hameçonnage<sup>1</sup>, APT et ingénierie sociale<sup>2</sup>. Ce type de renseignement est souvent regroupé avec le renseignement opérationnel sur les menaces. Cependant, il s'ajuste rapidement à mesure que les pirates informatiques mettent à jour leurs tactiques pour tirer parti de nouveaux événements et ruses.

- **Renseignements sur les menaces opérationnelles**

Avec cette approche, les informations sont collectées à partir de diverses sources, notamment les salles de discussion, les médias sociaux, les journaux antivirus et les événements passés. Ce renseignement est utilisé pour anticiper la nature et le calendrier des futures attaques. Exploration de données et apprentissage automatique sont souvent utilisés pour automatiser le traitement de centaines de milliers de points de données dans plusieurs langues. Les équipes de sécurité et de réponse aux incidents

---

<sup>1</sup> Phishing

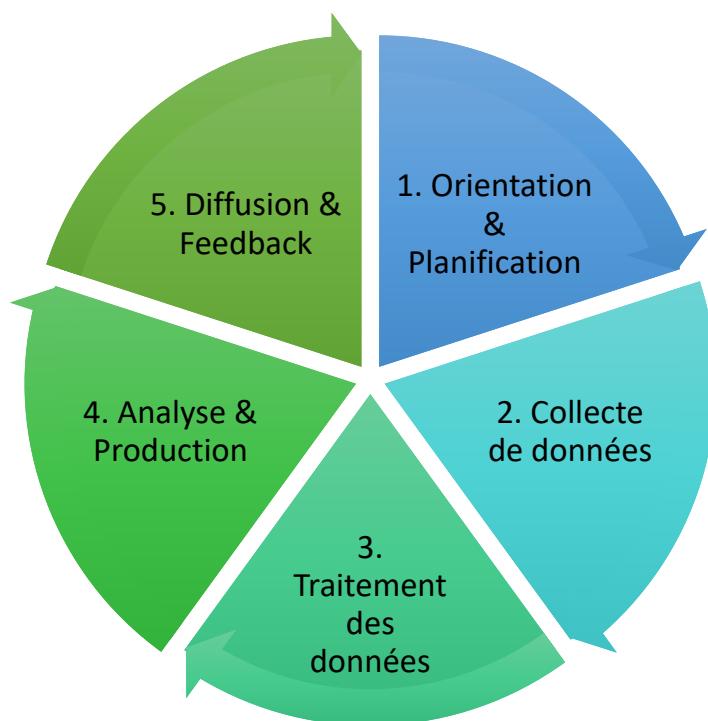
<sup>2</sup> Méthodes et techniques employées par les pirates et autres cybercriminels cherchant à tromper les victimes innocentes et leur faire partager leurs données personnelles (ex : ouvrir des liens vers des sites web infectés ou sans le savoir, permettre aux pirates d'installer des logiciels malveillants sur leurs ordinateurs, ...)

utilisent l'intelligence opérationnelle pour modifier la configuration de certains contrôles, tels que les règles de pare-feu, les règles de détection d'événements et les contrôles d'accès. Cela peut également améliorer les temps de réponse, car les informations fournissent une idée plus claire de ce qu'il faut rechercher.

## → Quel est le cycle de vie des renseignements sur les menaces?

Ce modèle vient du monde militaire, et il représente un cycle assez simple de création de renseignement. Ce cycle de renseignement reste une représentation logique, pragmatique et de bon sens de la façon de transformer les données et les informations. Ce qui aidera les décisions stratégiques et opérationnelles, ainsi à passer à l'action, réduire les risques et les incertitudes (dans le thème de la cybersécurité, détecter ou prévenir les attaques informatiques). Il s'agit d'un processus continu qui peut être répété indéfiniment. C'est aussi l'une des méthodes les plus importantes qui devraient guider le travail des analystes.

Dans le cycle du renseignement, traditionnellement il y a cinq étapes :



### 1. Orientation & Planification

Pour sélectionner les bonnes sources et outils de renseignements sur les menaces, une organisation doit décider ce qu'elle espère réaliser en ajoutant des renseignements sur les menaces à ses solutions et à sa stratégie de sécurité. L'objectif sera d'aider les équipes de sécurité de l'information à arrêter les menaces potentielles identifiées lors d'une modélisation des menaces exercer. Cela nécessite d'obtenir des données et des outils de renseignement qui peuvent fournir des conseils et des alertes

à jour sur les menaces considérées comme à haut risque et à fort impact. Un autre objectif important est de s'assurer que les bonnes informations stratégiques sont collectées et fournies à la direction afin qu'elle soit au courant des changements dans le paysage des menaces de l'organisation.

## **2. Collecte des données**

Les journaux des systèmes internes, contrôles de sécurité et les services cloud constituent la base du programme de renseignements sur les menaces d'une organisation. Cependant, pour obtenir des informations sur les derniers TTP et les informations spécifiques à l'industrie, il est nécessaire de collecter des données à partir de flux de données de menaces tiers. Ces sources incluent des informations recueillies sur internet, les journaux, de revues scientifiques, les adresses IP malveillantes, la télémétrie antivirus, de bases de données accessibles à tous, ...

## **3. Traitement des données**

La collecte et l'organisation des données brutes nécessaires à la création d'informations exploitables sur les menaces nécessitent un traitement automatisé. Il n'est pas viable de filtrer manuellement, d'ajouter des métadonnées<sup>1</sup>, de corrélérer et d'agréger divers types et sources de données. Les plates-formes ou application de renseignement sur les menaces utilisent l'apprentissage automatique pour automatiser la collecte et le traitement des données, afin de pouvoir fournir en permanence des informations sur les activités des acteurs de la menace.

## **4. Analyse & Production**

Cette étape consiste à trouver des réponses à partir des données traitées à des questions telles que quand, pourquoi et comment un événement suspect s'est produit.

## **5. Diffusion & Feedback**

Les rapports doivent être adaptés à un public spécifique afin qu'il soit clair comment les menaces couvertes affectent leurs domaines de responsabilité. Les rapports doivent être partagés avec la communauté au sens large lorsque cela est possible pour améliorer les opérations de sécurité globales.

Le temps pris pour faire le compte rendu de l'opportunité des renseignements reçus ou pour poser des questions n'est jamais un temps perdu. C'est l'occasion pour continuer à améliorer les missions.

---

<sup>1</sup> Caractéristiques formelles, normalisées et structurés utilisées pour décrire d'autres données.

## c. Évolution du logiciel Emotet

### → Qu'est-ce qu'Emotet?

Emotet est un cheval de Troie<sup>1</sup> qui cible des données bancaires. L'objectif de ce cheval de Troie est d'accéder aux appareils des personnes et d'espionner leurs données privées sensibles. Emotet est capable de tromper les programmes antivirus sans se faire détecter. Une fois l'appareil infecté, le programme se propage comme un ver informatique<sup>2</sup>.



Emotet se propage principalement via des spams. Ce mail contient un lien malveillant ou un document infecté. En cliquant sur le lien ou en téléchargeant le document, un autre malware se télécharge automatiquement sur l'appareil.

### → Le nom Emotet

Emotet a été détecté pour la première fois en 2014. Les cibles de ce cheval de Troie étaient les clients des banques allemandes et autrichiennes. Le programme est parvenu à accéder aux données de connexions des clients. Au fil du temps, ce programme s'est propagé dans le monde entier.

D'un cheval de Troie ciblant les données bancaires, Emotet est devenu un dropper<sup>3</sup>. Ce sont ces chevaux de Troie qui sont responsables des dégâts que nous rencontrons sur nos systèmes. Dans la plupart des cas, les programmes suivants ont été déposés :

1. **Trickbot** : cheval de Troie ciblant les données bancaires, qui tente d'accéder aux données des connexions des comptes bancaires.
2. **Ryuk** : cheval de Troie de chiffrement, également appelé ransomware<sup>4</sup> (ou cryptotrojan).

---

1 C'est un programme malveillant utilisé pour infecter le système PC cible et causer l'activité malveillante pour voler des informations personnelles.

2 Logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet.

3 Dropper (anglais) une forme minimaliste du cheval de Troie, appelé programme seringue ou virus compte-gouttes est un programme informatique créé pour installer un logiciel malveillant comme cible.

4 Rançongiciel (français) est un logiciel informatique malveillant, prenant en otage les données.

## → Qui Emotet cible-t-il ?

Au début, Emotet ciblait principalement des entreprises, alors que maintenant il vise majoritairement les particuliers. De nombreuses entreprises n'ont pas voulu signaler par crainte de salir leurs réputations mais aussi de faire l'objet de nouvelles attaques.

## → Quels sont les appareils exposés à Emotet ?

Ce cheval de Troie étaient uniquement détectées sur les systèmes d'exploitation les plus récentes de Windows. Au début de 2019, les chercheurs l'ont découvert sur les ordinateurs Apple. Grâce à un email frauduleux, les attaquants piégeaient les utilisateurs. L'email indiquait que l'entreprise avait « restreint l'accès à son compte ». Les victimes ont cliqué sur le lien pour éviter la désactivation de leurs comptes et la suppression de leurs services Apple.

## → Comment se propage-t-il ?

Emotet fait une collecte Outlook. Il lit les emails des utilisateurs déjà affectés et crée un contenu faussement authentique. Emotet envoie ces mails de phishing aux cibles. Généralement, les emails contiennent un lien ou un document Word dangereux que le destinataire est supposé télécharger. Les destinataires sont ainsi aveuglés par un faux sentiment de sécurité car ce mail semble parfaitement normal.

Une fois qu'Emotet a accès au réseau, il peut se propager tranquillement. Il essaie de trouver les mots de passe à l'aide de la méthode de force brute<sup>1</sup>. Une autre méthode qui figure les vulnérabilités sous Windows, autorisent l'installation du programme malveillant sans intervention humaine.

## → Un programme malveillant particulièrement destructeur

Le département de la Sécurité intérieure des États-Unis en est venu à la conclusion qu'Emotet était un logiciel particulièrement coûteux, doté d'une puissance destructrice phénoménale. Le coût du nettoyage est estimé à près d'un million de dollars par incident. Ce n'est pas pour rien qu'Arne SCHOENBOHM (directeur du BSI (en Allemand, Bundesamt für Sicherheit in der Informationstechnik)) appelle ce logiciel « Le Roi des programmes malveillant ».

Il y a 2 types de risques :

- Internes : phishing ciblant les collaborateurs
- Externes : phishing ciblant les clients.

---

<sup>1</sup> Méthode pour trouver le mot de passe ou la clé cryptographique afin de pouvoir accéder à un service en ligne, à des données personnelles ou un ordinateur.

Chez BNPP, chaque collaborateur à son propre PC et Téléphone Portable professionnelle. Seuls les membres de BNP peuvent communiquer entre eux. Lorsqu'ils reçoivent un mail externe, leurs messageries affichent « [EXTERNAL] ». Si ce mail externe contient un fichier ou un lien malicieux, ce mail est envoyé à l'équipe CSIRT pour vérifier s'il s'agit bien d'un phishing et prendre les mesures ci-nécessaires.

Les cybercriminels jouent plus sur les peurs de la population. Par exemple, un client d'Amazon ayant payés sa commande, reçoit un mail frauduleux, l'informant qu'il peut se faire rembourser. Le mail contenant un lien dangereux, va emmener la victime à cliquer sur le lien pour se faire rembourser. Lorsque la personne va rentrer ses données bancaires, le fraudeur va les récupérer et faire des virements à sa guise. Via l'application BNPP, lorsqu'il y a une activité anormale, le client recevra donc un mail en l'alertant d'être prudent. Le phishing peut cibler aussi les employés comme les clients.

Emotet est le programme le plus complexe et le plus dangereux de l'histoire de la cybercriminalité. Le virus est polymorphe<sup>1</sup>. En février 2020, les chercheurs de Binary Search ont découvert qu'Emotet attaquait désormais les réseaux Wi-Fi. Si un appareil infecté est connecté à un réseau Wi-Fi, Emotet analyse l'ensemble des réseaux situés à proximité. Au moyen d'une liste de mots de passe, le virus tente ensuite d'accéder aux réseaux et d'infecter d'autres appareils.

## → L'infrastructure du programme malveillant réduite à néant

À la fin du mois de janvier 2021, le Bureau du Procureur général de Francfort – le bureau central de la lutte contre la cybercriminalité – et le Bureau Fédéral des affaires criminelles (Federal Criminal Office, FCO) ont annoncé qu'Emotet avait été « contrôlée et détruite » dans le cadre d'un effort international. Les forces de l'ordre d'Allemagne, des Pays-Bas, d'Ukraine, de France et de la Lituanie, ainsi que le Royaume-Uni, le Canada et les États-Unis ont participé à l'opération. Les autorités affirment qu'elles sont parvenues à désactiver plus de 100 serveurs de l'infrastructure d'Emotet, dont 17 se trouvaient en Allemagne. La FCO a compilé des données et localisé après les analyses davantage de serveurs dispersés en Europe.

Selon le FCO, l'infrastructure du programme malveillant Emotet a été anéantie et mise hors d'état de nuire. Les autorités ukrainiennes ont été en mesure de prendre le contrôle de l'infrastructure et ont saisi de nombreux ordinateurs et disques, de l'argent et des lingots d'or. L'opération dans son ensemble a été coordonnée par Europol et Eurojust, l'organisme de l'Union européenne de coordination juridique pour la gestion des affaires criminelles.

En prenant le contrôle, les autorités ont réussi à rendre les systèmes affectés des victimes allemandes inutilisables par les auteurs de l'attaque. Pour les empêcher de reprendre le contrôle, les forces opérationnelles ont placé en quarantaine le programme malveillant sur les systèmes affectés des victimes.

---

<sup>1</sup> Son code change légèrement à chaque fois qu'il y a un accès.

## → Le retour d'Emotet en Novembre 2021

Divers experts en cybersécurité ont indiqué un regain d'activité du logiciel malveillant Emotet en novembre 2021. L'alerte a notamment été donné par Cryptolaemus, un groupe de chercheurs en sécurité qui s'est spécialisé dans la lutte contre Emotet.

Cryptolaemus explique qu'une nouvelle version d'Emotet a été observée et qu'elle utilise particulièrement des machines qui s'étaient autrefois retrouvées infectées par un autre malware, Trickbot<sup>1</sup>. Les sociétés GData et Advanced Intel ont ensuite confirmé et élaboré.

Elles estiment que si le « nouveau Emotet » est évidemment très proche de l'original, il intègre aussi de nombreuses différences qui contribuent à renforcer son efficacité. Il est ainsi question d'utiliser un système de chiffrement HTTPS pour assurer le trafic entre le malware et les serveurs de contrôle.

Les chercheurs de Cryptolaemus ont en outre souligné que la *commande buffe2<sup>2</sup>* est plus complexe qu'autrefois : « Nous pouvons maintenant confirmer que le command buffer a été modifié. Il comporte à présent 7 commandes contre 3-4 sur les précédents versions ».

Cryptolaemus précise avoir observé de larges campagnes de courriers électroniques « suspects » destinés à propager Emotet afin que les machines soient infectées par le malware. Sans surprise, il s'agit encore et toujours d'un des moyens privilégiés pour répandre son code.

Ces campagnes d'emails permettent d'infecter de nombreuses machines qui, après avoir contacté un serveur de contrôle du botnet<sup>3</sup>, peuvent à leur tour diffuser le logiciel malveillant. L'idée est, bien sûr, de reconstruire un vaste réseau de machines infectées, aux quatre coins de la planète.

En automne 2020, la France avait été une des cibles privilégiées des attaques Emotet. Avant l'intervention des différentes forces de police en début d'année 2021, Emotet était l'un des botnets les plus répandus et ont estimé à plus de 1,6 millions le nombre de machines infectées par ce malware.

À l'aide des contacts et fil de discussion récupérés précédemment, Emotet a pu automatiser la création de mails de phishing plus personnalisés. Ces emails se faisaient passer pour une réponse à un fil précédent entre la victime et l'un de ses

---

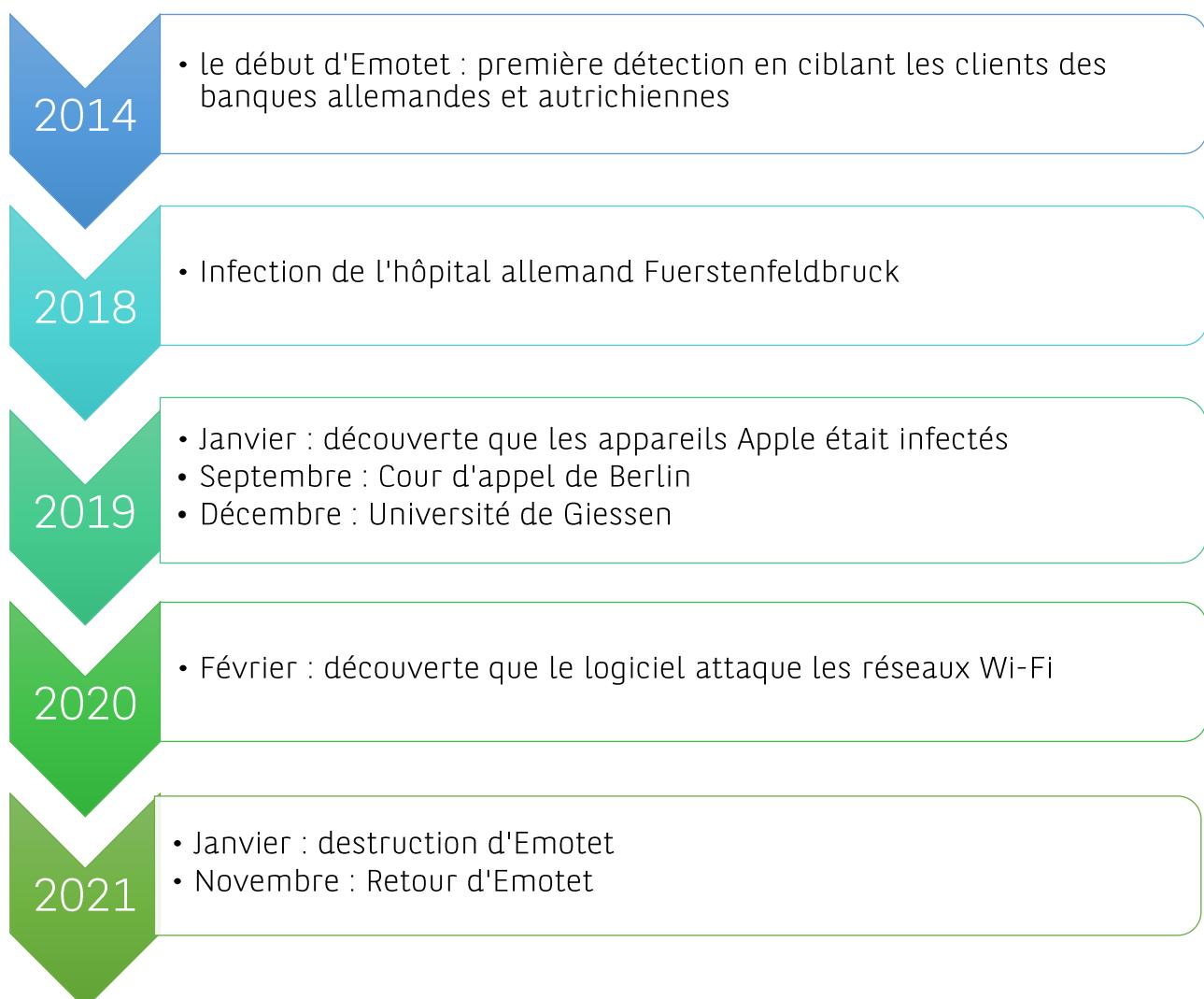
<sup>1</sup> Cheval de Troie ciblant les données bancaires, qui tente d'accéder aux données des connexions des comptes bancaires.

<sup>2</sup> Mémoire tampon en français, une zone de mémoire virtuelle ou de disque dur utilisée pour stocker temporairement des données, notamment entre deux processus ou deux pièces d'équipements ne fonctionnant pas à la même vitesse.

<sup>3</sup> Contraction de l'anglais (« ro bot net » : « réseau de robots ») qui est un réseau de bots informatiques, des programmes connectés à Internet qui communiquent avec d'autres programmes similaires pour l'exécution de certaines tâches.

contacts en mettant dans le corps du mail les anciennes discussions récupérées lors de l'attaque et en gardant l même sujet de mail auquel était ajouté le préfixe « Re : ». Dans certains cas, les anciennes pièces jointes étaient également ajoutées pour plus de légitimité. Cependant, ces emails n'étaient pas envoyés à partir de l'adresse mail compromise mais à partir de l'infrastructure des attaquants et d'adresses créées pour l'occasion et typosquées<sup>1</sup>.

#### **d. Frise chronologique d'Emotet**



<sup>1</sup> Type d'attaque d'ingénierie sociale qui vise les internautes qui tapent incorrectement une URL dans leur navigateur web plutôt que d'utiliser un moteur de recherche (connu aussi sous le nom de détournement d'URL, d'imitation de domaine, de sites piégés ou de fausses URL).

## VI. SYNTHESE

Il va de soi que la différence entre le monde de l'école et celui de l'entreprise est très importante. Ce stage de 4 semaines au sein du groupe SOC et sur un site aussi important m'a permis de découvrir la réalité du monde cyber.

L'accueil de l'entreprise de BNP Paribas étant bien préparé et détendu, cela m'a mis immédiatement en confiance avec l'équipe. D'autant plus que mes tuteurs de stage m'ont apporté toute l'aide dont j'avais besoin. Une bonne ambiance règne dans l'équipe et tous les personnels ont été très coopératifs et attentif à toutes mes questions. Le travail d'équipe est très important car tous les services sont liés et doivent communiquer entre eux.

Cette expérience est enrichissante tant du côté technique que du côté humain : c'était l'occasion de mener des projets, d'une manière totalement autonome avec une liberté de choix ainsi que d'acquérir des responsabilités, des connaissances, des capacités d'organisation, d'être précis et efficace et surtout constater des rapports humains.

Je remercie une fois de plus toutes les personnes que j'ai rencontrées pour m'avoir permis de mener à bien mes projets et de m'avoir accordé leurs confiances et leur sympathie durant cette période de stage.

# VII. ANNEXES



## ATTESTATION DE PFMP

Conformément à l'article D. 124-9 du code de l'éducation, une attestation de stage est délivrée par l'organisme d'accueil à tout élève. Ce document doit être complété et signé le dernier jour de la période de formation en milieu professionnel par un responsable autorisé de l'entreprise d'accueil et remis au stagiaire en deux exemplaires.

L'entreprise (ou l'organisme d'accueil) :

Nom : BNP PARIBAS

Adresse : 16 BD DES ITALIENS 59 Rue de la République  
75009-PARIS-9  
93-100 Montreuil

N° Siret : 66204244900014

Représenté(e) par :

Fonction :

Atteste que l'élève désigné ci-dessous :

Prénom : Hariharani Nom : THEIVENDRAM Date de naissance : 25 / 01 / 2005

Classe : Première BAC PRO RISC3

Diplôme préparé : BAC PRO SN OPTION RESEAUX INFORMATIQUES ET SYSTEMES COMMUNIQUANTS

Période n° 1 du 22 novembre 2021 au 18 décembre 2021 soit 20 jours\*

Scolarisé dans l'établissement ci-après :

LP GUSTAVE FERRIE

Représenté par la chef d'établissement, M. ANNE, proviseur.

Adresse : 7 rue des Ecluses Saint Martin - 75010 Paris

N° Tel : 01 42 02 19 55 N° Fax : 01 42 02 90 81

Email : ce.0750775k@ac-paris.fr

a effectué une période de formation en milieu professionnel dans notre entreprise ou organisme,

Soit une durée effective totale de :

Conformément à l'article D.124-6 du code de l'éducation, «Chaque période au moins égale à sept heures de présence, consécutives ou non, est considérée comme équivalente à un jour et chaque période au moins égale à vingt-deux jours de présence, consécutifs ou non, est considérée comme équivalente à un mois»

Le montant total de € a été versé au stagiaire à titre de gratification.

Fait à Montreuil, le 16/12/2021

Signature et cachet de l'entreprise ou de l'organisme d'accueil

\* Conformément à l'article D.124-6 du code de l'éducation, «Chaque période au moins égale à sept heures de présence, consécutives ou non, est considérée comme équivalente à un jour et chaque période au moins égale à vingt-deux jours de présence, consécutifs ou non, est considérée comme équivalente à un mois»

# EVALUATION PROFESSIONNELLE DES MISSIONS EN STAGE



IDENTIFICATION

CONTEXTE

APPROBATION DES MISSIONS EN STAGE

Nom : THEIVENDRAM	Date de l'évaluation : 13/12/2021
Prénom : Hariharani	Identifiant : e53771
Entité : SOC - ITRMG Security Operation Center	Dates du stage : du 22/11/2021 au 18/12/2021
Formation académique suivie : BAC PROF SYSTEMES NUMERIQUES	Mission occupée :
Type de stage : Stage de 1 <sup>re</sup>	Lieu de la mission : Valmy 1, Montreuil
Nom du Tuteur Entreprise : Patria AZZAM	

## Eléments de contexte

Hariharani est une élève de première au Lycée Professionnel Gustave Ferrié et elle a effectué un stage d'un mois chez BNPP au sein du Groupe SOC (IT Groupe - ITRMG). Ce stage, ainsi que 3 autres, sont obligatoires pour l'acquisition de son bac.

## Missions réalisées au cours de la période de stage

Missions	Découverte de l'entreprise et de l'environnement	4	Appréciations
	Découverte des différentes activités du SOC (réponse à incident, threat intelligence, phishing, cyber-fraud, etc.)	4	
	Focalisation sur ce que c'est la Cyber Threat Intelligence	3	
	Synthèse de l'histoire du malware qui s'appelle « Emotet »	4	
	Rédaction de son rapport de stage	4	

1-Exercé de façon exceptionnelle, 2-Exercé très au-delà des attendus du poste, 3-Exercé au-delà des attendus du poste, 4-Exercé conformément aux attendus du poste, 5-Partiellement exercé, 6-Insuffisamment exercé

## Compétences liées à la mission

Les mieux maîtrisées (1 à 3)	A développer (1 à 3)
Sérieuse	Synthèse
Curieuse	



**BNP PARIBAS**

La banque  
d'un monde  
qui change

SYNTHESE

## Commentaires du Tuteur Entreprise

Hahirani est sérieuse dans son travail. Elle a pu profiter de sa présence en entreprise pour comprendre l'environnement et les différentes activités afin de se projeter dans son futur projet professionnel. Elle a passé du temps pour mieux appréhender le sujet de la « Cyber Threat Intelligence » et lire des articles sur internet sur le malware « Emotet » afin de rédiger une synthèse de ce qu'elle a compris. Elle a soigneusement travaillé son rapport de stage afin qu'il réponde au cahier de charge de son lycée.

## Recommanderiez-vous le recrutement de ce stagiaire au sein du Groupe ? Si oui, sur quel type de mission ou de poste ?

N/A

## Commentaires du stagiaire

Ce stage de 4 semaines au sein du groupe SOC, m'a permis de découvrir la réalité du monde cyber. Une bonne ambiance règne dans l'équipe et tous les personnels ont été très coopératifs et attentif à toutes mes questions. Je remercie infiniment, M. RIGHI, M. CIRACQ et Mme. AZZAM de m'avoir donnée l'opportunité de réalisé ce stage dans des conditions agréable. Je remercie une fois de plus toutes les personnes que j'ai rencontrées pour m'avoir permis de mener à bien mes projets et de m'avoir accordé leurs confiances et leur sympathie durant cette période de stage.

### Date, Nom et signature du tuteur

13/12/2021  
Patria AZZAM



### Date et signature du collaborateur

13/12/2021  
Hariharani THEIVENDRAM



### Date, Nom et signature du Responsable Formation (Pour BDDF Réseau/ RGRH)



**BNP PARIBAS**

La banque  
d'un monde  
qui change

## **VIII. CONSEILS**

## a. Sites actualités cyber

ANSSI - [Agence nationale de la sécurité des systèmes d'information \(ssi.gouv.fr\)](http://Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr))

Feedly - [Welcome to Feedly](#)

Nolimitsecu - [NoLimitSecu](#) - Podcast dédié à la cyber sécurité

EuroPol - [Home](#) | [Europol \(europa.eu\)](#)

InterPol - [INTERPOL | L'Organisation internationale de police criminelle](#)

Enisa - [ENISA \(europa.eu\)](http://enisa.europa.eu)

Cybermalveillance.gouv.fr - [Assistance aux victimes de cybermalveillance](#)

Kaspersky - [Solutions de cybersécurité Kaspersky pour les particuliers et les entreprises](#) | Kaspersky

Whatis.com - Computer Glossary, Computer Terms - Technology Definitions and Cheat Sheets from WhatIs.com - The Tech Dictionary and IT Encyclopedia ([techtarget.com](http://techtarget.com))

ProofPoint - [Enterprise Cybersecurity Solutions, Services & Training | Proofpoint US](#)

Cyberchef - [CyberChef \(gchq.github.io\)](https://gchq.github.io/CyberChef/)

Cyberwire daily - [Episodes of CyberWire Daily](#) | Podchaser

## b. Ecole

EGE Paris 7<sup>e</sup> - [https://programmes.ege.fr/ ecole-de-guerre-economique-cybersecurite/?utm\\_content=I90705M0264&c=I90705M0264](https://programmes.ege.fr/ ecole-de-guerre-economique-cybersecurite/?utm_content=I90705M0264&c=I90705M0264)

ENSEIRB MATMECA BORDEAUX - [Bienvenue à l'ENSEIRB-MATMECA | ENSEIRB-MATMECA \(bordeaux-inp.fr\)](#)

ENSI BOURGES - [Institut National des Sciences Appliquées Centre Val de Loire \(insa-centrevaldeloire.fr\)](http://Institut National des Sciences Appliquées Centre Val de Loire (insa-centrevaldeloire.fr))

Cyber University Puteaux - [Formation en cybersécurité | Cyber University](#)