THEIVENDRAM Hariharani, 1R3

RAPPORT PFMP n°2

28 Mars au 22 Avril 2022

BACCALAUREAT PROFESSI0NNEL SYSTEMES NUMREIQUES
RISC (Réseaux Informatiques et Systèmes Communiquant)

Lycée Professionnel Gustave Ferrié

7 Rue des Ecluses St Martin, 75010 Paris

01 42 02 19 55

SOMMAIRE

I. REMERCIEMENTS

Il m’est agréable à remercier Mme. Patria AZZAM, ma mentor et collaborateurs en IT chez BNP Paribas et Youssef EL CADI IDRISSI, manager du groupe Network Security, pour m’avoir donnée l’opportunité de réaliser ce stage.

D’autre part, je remercie plus particulièrement M. Serge VONDANDAMO de m’avoir accueilli chaleureusement et M. Laurent RAYNAUD, mon tuteur de stage qui a tenu le rôle de guide durant cette insertion professionnelle. Je remercie également Meriam, une stagiaire de grande étude qui m’a aussi aidé durant ma période de stage. Ils ont tous 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 Network Security pour son soutien et son écoute, chacun a su rendre mon stage plus agréable et instructif.

Je remercie par ailleurs M. CLAVE, mon professeur référent ainsi que 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 28 mars au 22 avril 2022, j'ai effectué un stage au sein de l'entreprise BNP Paribas, située à Montreuil, que j'ai réalisé dans le département Network Security.

Plus largement, ce stage a été l'opportunité pour moi de comprendre mieux le monde de la sécurisation du réseau. Mon maître de stage étant très agréable, 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 la BNP Paribas, il paraît logique de présenter à titre préalable l'environnement informatique du stage, à voir le secteur du Telecom. Enfin, il sera précisé les différentes missions et tâches que j'ai pu effectuer ay sein du département, et les nombreux apports que j'ai pu en tirer.

III. PRESENTATION DE L'ENTREPRISE

a. Coordonnées

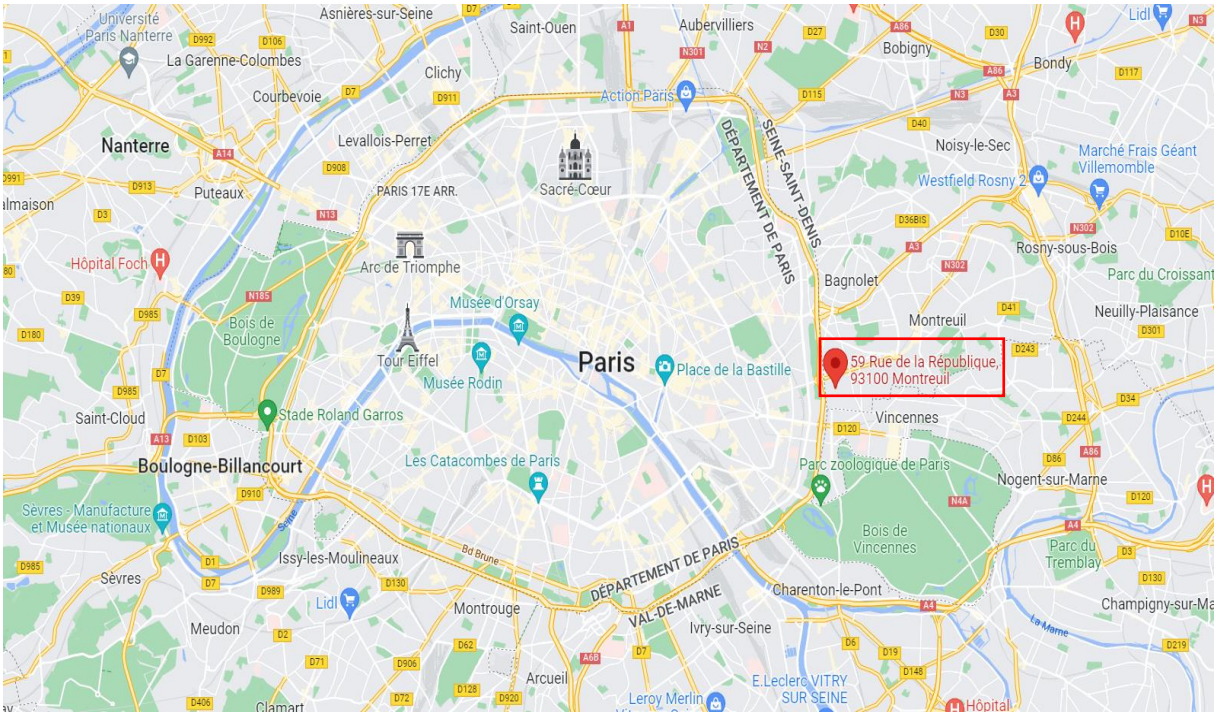
Nom : BNP Paribas – Valmy 1

Adresse : 59 Rue de la république, 93100 Montreuil

N° de téléphone : 06 33 30 36 66

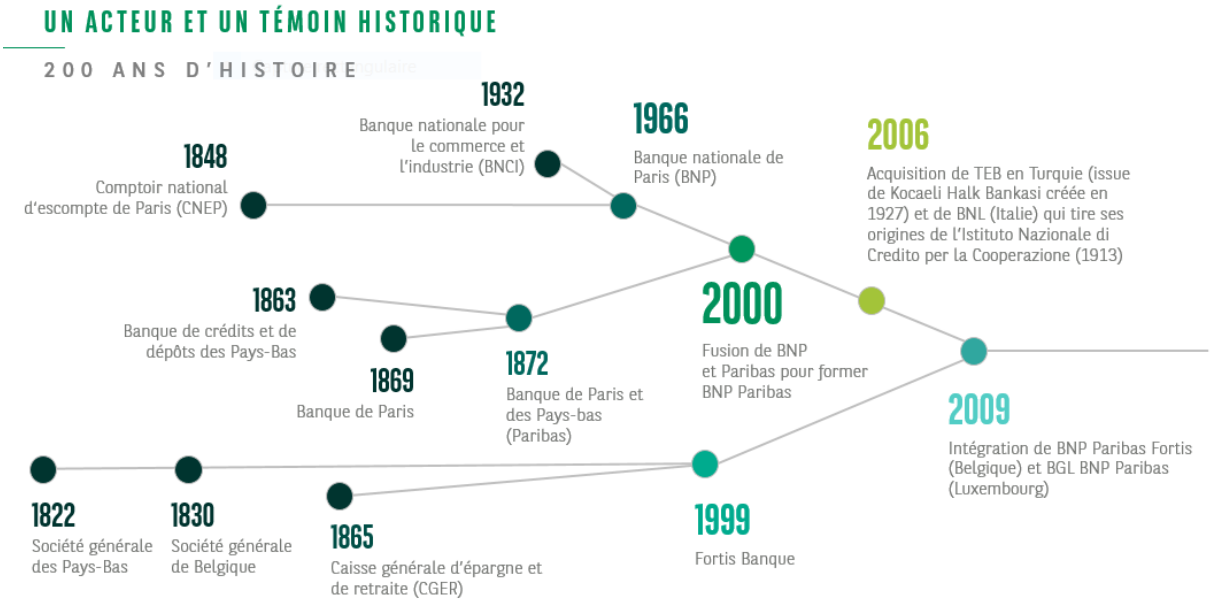
N° de Siret : 662 042 449 000 14

b. Situation géographique

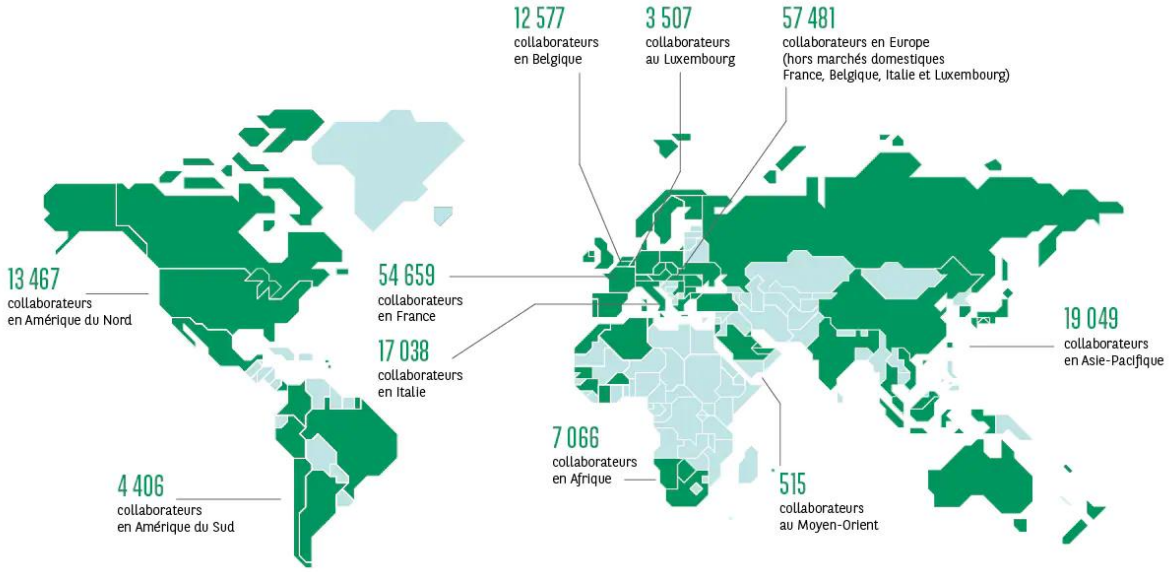


c. Histoire de BNP Paribas

L'histoire de BNP Paribas début au XIXème siècle, alors que les banques ancêtres du Groupe naissent et se développent. Entrainées par le formidables essor industriel de l'Europ, elles drainent l'épargne nécessaire au financement du développement économique. En remontant aux sources du Groupe, ce sont près de 25 siècles d'histoire du secteur de la banque, mais aussi d'histoire de l'Europe, voire du monde, que l'on peut parcourir.

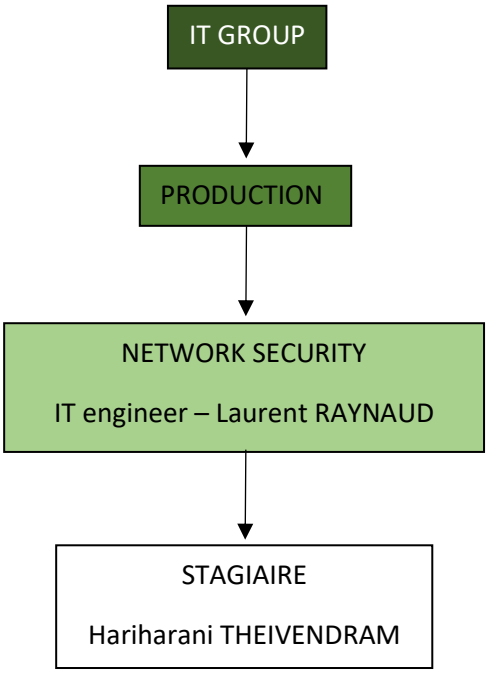


BNP Paribas est présent dans 68 pays avec plous de 193 000 collaborateurs dont près de 148 000 en Europe. Le groupe accompagne tous ses clients – particuliers, associations, entrepreneurs, grandes entreprises et institutionnels – dans la réussite de leurs projets grâce à ses solutions de financement,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



Partenaires (exemple)	Concurrents (exemple)
• Handisport • Festival Cinema • Etc.	• Société générale • Crédit agricole • Etc.

d. Organigramme de l'équipe



IV. COMPTE-RENDU D'ACTIVITES

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

Rencontres avec :

- Les membres de l'équipe Network Security.
- Les membres de l'équipe Browsing and Hosting.
- Les membres de l'équipe SDM (Service Delivery Management) ou bien Production.

Réunions :

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

- **Webinar :** une présentation sur le Zero-trust, qui est une nouvelle stratégie de sécurité. Elle adresse essentiellement les entreprises afin d'améliorer leur sécurité en changeant le rapport de confiance qu'elles ont en leur réseau et en y ajoutant/renforçant des points de contrôle d'accès.
- **Service Browsing :** C'est un service de navigation internet / intranet géré par du filtrage proxy (authentification, URL Filtering, Déchiffrement SSL, analyse anti-malware et DLP) pour assurer la sécurisation des flux Web utilisateurs et serveurs.

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 BNP Paribas 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.
- **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.**

En retirant le badge, la session se verrouille automatiquement. Il est préférable d'attacher un antivol au cas où il y a une intrusion malveillante.

3. **Ranger les documents confidentiels dans les placards et fermer à clefs.**

Si on a plus besoin de certains documents (papiers), il faut les détruire.

Au cours de mon stage, j'ai étudié divers sujets :

- **Les Firewalls** : Un Firewall est un appareil de sécurité réseau qui analysent soigneusement le trafic entrant en fonction de règles préétablies et filtrent le trafic provenant de sources non sécurisées ou suspectes pour empêcher les attaques. Les

firewalls contrôlent le trafic au point d'entrée d'un ordinateur, appelé port, qui est l'endroit où les informations sont échangées avec des appareils externes.

- **Le Browsing :** C'est un service de navigation internet / intranet géré par du filtrage proxy (authentification, URL Filtering, Déchiffrement SSL, analyse anti-malware et DLP) pour assurer la sécurisation des flux Web utilisateurs et serveurs.

- **Le Lab virtuelle** : c'est un laboratoire virtuel qui permet d'installer, configurer et tester des équipements.

- **La monétique :** c'est le chemin parcouru par la monnaie virtuelle.

- **La Chaine de la production** : C'est le cycle de la création d'une application par un métier (métier celui qui connait bien son travail).

V. ETUDES DE CAS

Les entreprises subissent de plus en plus d'attaques et les menaces viennent aussi bien de l'intérieur que de l'extérieur. Les acteurs malveillants utilisent les accès existants et piratent les périmètres. Une fois à l'intérieur, ils sont capables d'augmenter les niveaux des privilèges, d'effectuer des repérages et de se déplacer latéralement à l'intérieur du réseau, de perturber les activités et d'extraire des données. Le contexte actuel montre les limites du modèle traditionnel du château fort consistant à protéger le Système d'Information (SI) interne de l'entreprise.

En 2004, au Jericho Forum, sont élaborés les 'Network Access Control', initiant les débuts du Zero Trust. Puis en 2010, John KINDERVAG, ancien collaborateur de Forrester élabore le terme du Zero Trust qui veut dire : « *Ne jamais faire confiance, toujours vérifier* ». C'est un changement de vision qui passe d'un accès traditionnel basé sur le périmètre à un modèle axé sur l'utilisateur.

Le Zero Trust est une approche de sécurité intégrée pour les utilisateurs, les applications, les données et les réseaux qui nécessite des principes d'authentification forte et renforcée et l'utilisation de politiques d'accès.

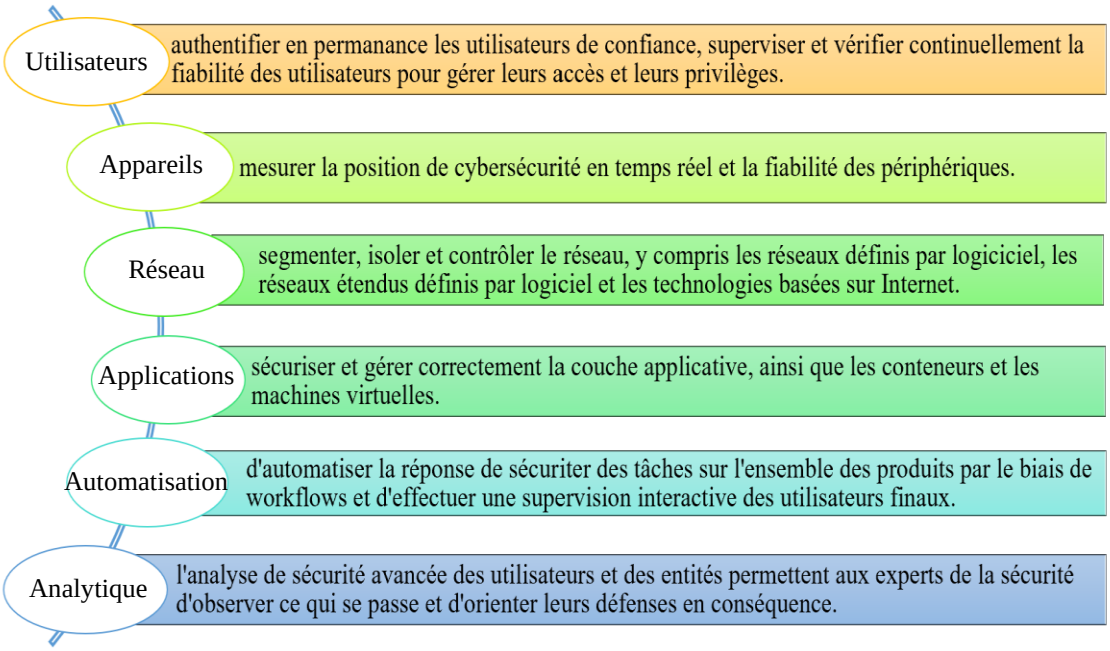
Chaque tentative d'accès aux systèmes est controlée comme si elle provenait d'un réseau non fiable, hostile. Ce modèle encourage l'utilisation des analyses avancées pour mieux détecter les menaces et les violations. Pour atteindre son efficacité maximale, les entreprises doivent commencer par l'identité de l'utilisateur. Il faut mettre en place une stratégie forte de gouvernance et d'administrions des identités. Lorsqu'elle sera correctement mise en œuvre, la solution offrira une visibilité permettant de **vérifier : qui accède à quoi, pourquoi, comment et d'où ?**

- **Qui :** utilisateurs et services (plus tard des ressources)
- **Quoi :** applications, qu'elles soient dans le cloud ou non
- **Pourquoi** : raison de l'accès, basée sur des règles spécifiées
- **Comment :** réseaux d'entreprise, et de plus en plus le réseau Internet
- **D'où :** équipement et sa localisation.

La gestion des accès est essentielle dans le modèle Zero trust. L'évaluation du contexte de l'identité au cours du processus d'authentification et d'autorisation permet de s'assurer qu'un utilisateur est bien celui qui prétend être, qu'il utilise l'appareil qu'il devrait utiliser et qu'il

accède au réseau depuis un lieu autorisé. L'identité définit et accorde l'accès que l'utilisateur devrait avoir et supprime tout accès qui n'est pas adapté, approprié ou dont il n'a plus besoin.

L'American Council for Technology and Industry Advisory Council (ACT-IAC), un partenariat public-privé à but non lucrative voué à l'amélioration du gouvernement par le biais des technologies de l'information, établit les six piliers du modèle Zero Trust. Ils se résument de la façon suivante :



Le confinement décrété en raison de la crise du Covid-19 par plusieurs gouvernements nationaux a obligé les entreprises à donner accès à leurs applications en dehors du réseau interne ou via des VPN. Les utilisateurs pouvaient se situer n'importe où, sans l'environnement sécuritaire requis. Ce bouleversement brutal, dont la date, le 17 mars 2020, restera dans toutes les mémoires, a obligé la plupart des entreprises à changer de paradigme pour la protection de leurs systèmes d'information et la sécurisation des accès.

Cette situation de travail à distance a généré des problèmes de sécurité, notamment pour accéder à des applications qui n'étaient pas forcément conçues pour être accessibles de l'extérieur du réseau de l'entreprise. Certaines entreprises ont atteint, voire dépassé, les limites de leur VPN, en particulier la limitation de la bande passante.

Dans ce contexte, de nombreuses organisations commencent à adapter leur fonctionnement au travail à distance et leur intérêt pour le concept de Zero Trust a progressé afin d'établir un lien de confiance entre l'utilisateur et la machine. Ce n'est pas parce que l'on a confiance à un collaborateur qu'on a confiance envers sa machine.

Problématique :

Que se passe-t-il lorsqu'on a volé ma carte bancaire ?

Etape 1 : Le voleur va surement utiliser le moyen de paiement SANS CONTACT.

Etape 2 : Au bout de 3 transactions, la carte ne pourra plus fonctionner en sans contact.

Etape 3 : Le voleur devra insérer la carte dans le terminal de paiement.

Etape 4 : Taper le code.

Etape 5 : Au bout de 3 essais, la carte sera bloquée et le porteur recevra un mail/SMS.

Cette problématique est liée avec le Zero Trust. Le paiement sans contact permet de passer la carte sans contact physique, c'est-à-dire sans taper le code confidentiel sur le terminal de commande. Le plafond de paiement sans contact par carte bancaire est relevé à 50€. Les établissements bancaires peuvent fixer un nombre maximum de transactions par jour. Une fois l'un de ces seuils atteints, pour réinitialiser vos plafonds, il faut effectuer une opération avec saisie du code confidentiel (un retrait ou un paiement). Ce code est la preuve pour que la carte puisse identifier et confirmer qu'il s'agit bien du porteur.

Lors de 3 essai, la carte sera bloqué bar une autre stratégie de sécurité, car il ne va pas identifier le vrai porteur de la carte.

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 Production Telecom et sur un site aussi important m'a permis de découvrir la réalité du monde de la sécurisation du réseau.

L'accueil de l'entreprise BNP Paribas étant bien préparé et détendu, cela m'a mis immédiatement en confiance avec l'équipe. D'autant plus que mon tuteur de stage m'a 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
75009 PARIS 9

N° Siret : 66204244900014

Représenté(e) par : Laurent RAYNAUD Fonction : Responsable d'équipe

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° 2 du 28 mars 2022 au ~~23~~ 22 avril 2022 soit ~~20~~ 19 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 0 € a été versé au stagiaire à titre de gratification.

Fait à Montreuil **, le** 21 avril 2022

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

RH&G Ressources Humaines Groupe

IDENTIFICATION

Nom : THEIVENDRAM
Prénom : Hariharani
Entité : Network Security
Formation académique suivie : BAC PRO SYSTEMES NUMERIQUES
Type de stage : Stage de 1ere
Nom du Tuteur Entreprise : Laurent RAYNAUD

Date de l'évaluation : 21/04/2021
Identifiant : e53771
Dates du stage : du 28/03/2022 au 22/04/2022
Mission occupée :
Lieu de la mission : Valmy 1, Montreuil

CONTEXTE

Eléments de contexte

Hariharani est une élève de première au Lycée Professionnel Gustave Ferrié et elle a effectué un second stage d'un mois chez BNPP au sein de l'équipe Network Security (IT Groupe – Production Telecom).
Ce stage fait partie des 4 stages nécessaires à l'obtention de son bac.

APPRECIATION/EVALUATION DE LA PERIODE ECOULEE

Missions réalisées au cours de la période de stage

Missions		Appréciations
Découverte de l'équipe Network Security et de ses activités, prise en main sur l'environnement informatique	4	
Etude théorique et compréhension sur la thématique Zéro Trust ainsi que les problématiques associées	4	
Maquettage d'un environnement en laboratoire pour découvrir et comprendre l'environnement technique	4	
Rédaction du rapport de stage associé	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)
Compréhension de l'environnement technique	Prise d'initiative
	Synthèse

BNP PARIBAS

La banque d'un monde qui change

EVALUATION PROFESSIONNELLE DES MISSIONS EN STAGE

RHG
Ressources Humaines Groupe

SYNTHESE

Commentaires du Tuteur Entreprise

Hariharani a intégré cette mission dans un contexte particulier (j'étais personnellement positif au covid-19) et la prise en main du sujet et des attendus n'ont, de ce fait, pas été aussi simple que prévu.
Elle a assisté aux différentes sessions sur le Zero Trust et suivi un e-Learning du Groupe sur la sécurité des systèmes, s'est intéressé à la réalisation d'un lab pour comprendre à la fois l'environnement technique sur lequel l'équipe intervient et le lien avec son étude théorique (Zéro Trust).

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

NA

Commentaires du stagiaire

Ce stage de 4 semaines au sein du groupe Network Security, m'a permis de découvrir la réalité du monde de la sécurisation. J'ai pu apprendre de nouvelles choses comme le Zero-Trust, la monétique, etc. même dans un délai très court. Une bonne ambiance règne dans l'équipe et tous les personnels ont été très agréable. Je remercie Laurent RAYNAUD de m'avoir donné l'opportunité de réalisé ce stage dans de bonnes conditions. 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 temps, leurs confiances et leur sympathie durant cette période de stage.

Date, Nom et signature du tuteur

22/04/2022
Laurent RAYNAUD

Date et signature du collaborateur

22/04/2022

Date, Nom et signature du Manager (uniquement si budget pour recruter sur le poste actuel)

BNP PARIBAS

La banque
d'un monde
qui change