

ENSEIGNANT RÉFÉRANT: MADAME GALEA
TUTEUR DE STAGE: DAMIEN RAYNAL

ANTONIN NICOLAS

LE MONDE DE LA CYBERSÉCURITÉ

2021 / 2022

DU 31 JANVIER AU 4 FÉVRIER 2022

RAPPORT DE STAGE

ENTREPRISE D'ACCUEIL: PALO ALTO NETWORKS - 62 AVENUE ÉMILE ZOLA
IMMEUBLE A, 92100 BOULOGNE-BILLANCOURT

ÉTABLISSEMENT: STANISLAS CANNES - 1 PLACE STANISLAS, 06400 CANNES

ENSEIGNANT RÉFÉRANT: MADAME GALEA

TUTEUR DE STAGE: DAMIEN RAYNAL

ANTONIN NICOLAS

LE MONDE DE LA CYBERSÉCURITÉ

2021 / 2022

DU 31 JANVIER AU 4 FÉVRIER 2022

RAPPORT DE STAGE



ENTREPRISE D'ACCUEIL: PALO ALTO NETWORKS - 62 AVENUE ÉMILE ZOLA
IMMEUBLE A, 92100 BOULOGNE-BILLANCOURT

ÉTABLISSEMENT: STANISLAS CANNES - 1 PLACE STANISLAS, 06400 CANNES

Auteur : Antonin NICOLAS

Conception graphique : réalisée sur Canva

Mise en page : réalisée sur Word

Achevé d'imprimer le 19 février 2022

Source image de la couverture et de la 4eme de couverture :

<https://www.facilogi.com/blog/cybersecurite-dans-limmobilier/> – Les professionnels de l'immobilier et les cyber-risques – 27 novembre 2019

Source image des pages de nouveaux chapitres :

<https://fr.linkedin.com/company/id-informatique> – ID Informatique – Développement de logiciels

TABLE DES MATIÈRES

I. PRÉAMBULE	
Remerciements.....	7
Lettre de motivation.....	8
Introduction.....	9
II. L'ENTREPRISE	
Historique et situation géographique.....	11
Organisation et services.....	11
Une petite description.....	11
En quoi consiste son activité ?.....	12
III. MON SÉJOUR	
Lundi.....	15
Mardi.....	16
Mercredi.....	17
Jeudi.....	18
Vendredi.....	19
IV. DÉCOUVERTES	
Présentation du principal métier observé.....	21
Les 6 autres professions.....	22
V. IMPRESSIONS	
Ce que j'imaginais avant le stage et ce que j'ai pu observer.....	27
Est-ce une expérience intéressante ?.....	28
Une aide pour mon projet professionnel ?.....	29
Conclusion.....	30
VI. ANNEXES	
Bibliographie.....	37

PRÉAMBULE

- REMERCIEMENTS
- LETTRE DE MOTIVATION
- INTRODUCTION

Remerciements

Je ne pourrais pas commencer la rédaction de ce rapport sans remercier monsieur **Damien RAYNAL**, tout d'abord pour son accueil au sein de son département et de sa société mais aussi pour tout ce qu'il a pu m'apporter pendant cette semaine de stage à ses côtés. Ses conseils avisés m'ont permis de beaucoup apprendre sur le fonctionnement de l'entreprise et d'acquérir de nouvelles connaissances et compétences. Je le remercie également pour la confiance qu'il a su m'accorder dès les premiers instants.

Je remercie également l'ensemble des personnes avec qui j'ai pu travailler ou que j'ai pu interviewer afin d'avoir une vision approfondie des métiers clés d'une société. Ils ont su se rendre disponibles quand cela était nécessaire et ont toujours pris soin de m'expliquer les choses de façon pédagogique.

Enfin, je souhaite remercier le relecteur qui a su contribuer, grâce à ses conseils et recommandations, à l'élaboration et au bon déroulé de mon rapport de stage.

Lettre de motivation

7 novembre 2021

Damien Raynal

Director system engineer

Palo Alto Networks

ant.nicolas@stanislas-cannes.com

62 avenue Emile Zola immeuble A

Boulogne-Billancourt, 92100

Monsieur Raynal,

Le programme scolaire des collégiens en année de troisième prévoit une période de stage en entreprise de une semaine, dont la vocation est de permettre aux élèves de découvrir le monde professionnel et d'acquérir une première expérience.

Dans ce cadre, je souhaite pouvoir effectuer ce stage, du 31 janvier au 4 février, au sein de votre entreprise.

Intéressé par votre secteur d'activité, j'envisage de devenir ingénieur en cybersécurité. Cette immersion serait ainsi l'occasion de me familiariser avec le monde de l'entreprise, mais également d'approfondir mes connaissances sur le métier d'ingénieur, et ainsi de confirmer mes futurs choix d'orientation.

Sérieux, ponctuel et discret, je pourrai observer le fonctionnement de votre entreprise sans en gêner l'organisation, et aussi vous aider dans la réalisation de certaines tâches.

Je vous remercie par avance de l'intérêt que vous porterez à ma demande, et me tiens à votre disposition. En espérant avoir un retour positif de votre part, je serais ravi de pouvoir vous expliquer plus en détails mes motivations à l'occasion d'un éventuel rendez-vous.

Dans cette attente, je vous prie d'agréer, Monsieur, l'expression de mes sincères salutations.

Bien cordialement,

Antonin NICOLAS

Introduction

Avec des milliards d'appareils connectés, de nouvelles menaces informatiques surgissent chaque seconde (une cyber-attaque se produit toutes les 11 secondes) et la demande en cyber-défenseurs demeure très élevée. Au cœur des enjeux de sécurisation de la société numérique et en matière d'innovation, la cybersécurité devrait tirer parti des recherches dans le domaine des mégadonnées (big data) qui combineront apprentissage automatique et intelligence artificielle.

Ce stage me permettra d'avoir une vue d'ensemble et précise des métiers de la cybersécurité. Je suis assez anxieux à l'idée de découvrir les métiers de l'informatique et leurs rôles dans l'entreprise Palo Alto Networks car cela ne sera sûrement pas ce que l'on imagine. Ce sera la réalité.

J'ai choisi ce stage car je souhaite orienter mon projet professionnel vers l'informatique et plus localement la cybersécurité. Dans mon cas, il n'y a pas d'entreprise plus adaptée que le leader mondial actuel de la cybersécurité, Palo Alto Networks. À ce titre, ils ont le privilège d'assurer la sécurité de dizaines de milliers d'entreprises.

Ce stage sera donc une opportunité pour moi de percevoir comment une entreprise dans le secteur de la cybersécurité se développe en contexte international, ses défis et son évolution au cours du temps. L'élaboration de ce rapport a pour principale source les différents enseignements tirés de la pratique journalière des tâches auxquelles j'ai été confronté. Enfin, les nombreux entretiens que j'ai pu avoir avec les employés des différents services de la société m'ont permis de donner une logique à ce rapport.

En vue de rendre compte de manière fidèle et analytique la semaine passée au sein de la société Palo Alto Networks, il apparaît logique de présenter à titre préalable la société dans laquelle j'ai été accepté et ses activités, puis d'envisager le cadre du séjour au sein de celle-ci ainsi que les tâches que j'ai pu effectuer. Ensuite, il sera précisé les différents métiers que j'ai découvert au sein des services d'avant-vente, de vente et de mise en œuvre, et les nombreuses impressions que j'ai pu en tirer.

L'ENTREPRISE

- HISTORIQUE ET SITUATION GÉOGRAPHIQUE
- ORGANISATION ET SERVICES
- UNE PETITE DESCRIPTION
- EN QUOI CONSISTE SON ACTIVITÉ ?

Historique et Situation géographique

Palo Alto Networks a été fondée en 2005 par Nir Zuk qui occupe actuellement le poste de directeur et chef de la technologie chez Palo Alto. Il a précédemment occupé le poste de technologue en chef de la sécurité chez Juniper Networks, directeur de la technologie chez NetScreen Technologies, Inc. et directeur de la technologie chez OneSecure dont il est lui-même l'auteur (toutes deux filiales de Juniper Networks).

Quant à Palo Alto dont le siège social est installé à Santa Clara (Californie, USA), sa technologie a su révolutionner le monde de la sécurité informatique grâce à une nouvelle génération de firewall assurant une précision et un contrôle inédit, notamment au niveau des applications et du contenu. Ainsi, elle s'est développée pour devenir le leader mondial de la cybersécurité. Aujourd'hui, elle permet à plus de 75 000 entreprises dans 150 pays de protéger des cyber failles les données de plusieurs milliards de personnes dans le monde. Cela a eu pour conséquence de faire un chiffre d'affaire supérieur à 5 millions de dollars américains en 2021. Cela donne une évolution de près de 25% par rapport à celui de 2020. ([voir annexe 1](#))

Organisation et services

Conscient que leurs clients ont beaucoup trop d'interlocuteurs sécurités, ce qui conduit bien souvent à complexifier le travail, la société propose des solutions reposant sur des services transverses, délivrés depuis le cloud afin d'assurer une homogénéité tout en tenant compte des spécificités des environnements de chaque client.

La plateforme de sécurité de Palo Alto Networks peut alors être schématiquement découpé en 3 piliers² ([voir annexe 2](#)):

Strata s'appuie sur le meilleur firewall nouvelle génération du marché auquel s'intègrent des innovations constantes sous forme de souscription.

Prisma gère tous les scenarii de sécurisation du cloud. De l'accès vers le cloud où que soit l'utilisateur jusqu'au contrôle de l'accès aux ressources dans tous les clouds.

Cortex présente une suite de produits pour la sécurité opérationnelle, avec une offre de prévention, automatisation, détection et réponse. Cortex agit sur le réseau, les endpoints (fin d'un cycle) et le cloud.

Une petite description

Nous vivons dans l'ère de la transformation numérique, la transformation digitale (digitalisation) où nos échanges sont de plus en plus rapides. L'accès universel à l'information, et la migration du support de l'information permet à de nombreuses personnes de s'enrichir intellectuellement. Malheureusement de nouveaux challenges

s'adressent à nous, et la cybersécurité de l'information en fait partie.

Aujourd'hui Internet est devenu notre moyen de communication privilégié, le cloud est devenu notre datacenter, notre bureau est indifféremment chez nous, dans l'entreprise. La puissance de traitement, le volume de données sont illimités grâce aux géants du web (Google, Amazon, Microsoft, Facebook, etc..) et le nombre de services augmentent exponentiellement. L'intelligence artificielle et le machine learning qui s'appuient sur cette puissance du cloud favorisent une automatisation des tâches qui devient nécessaire pour accélérer les temps de réponses aux prises de décisions quelle qu'elle soit .

Cette révolution numérique modifie aussi le paradigme des cyberattaquants, de la même façon. Les attaquants se servent de l'automatisation pour rapidement transformer leurs attaques, contourner les protections traditionnelles. Les nouveaux appareils, les objets connectés qui doivent être protégés prolifèrent vite en silence.

En plus des applications qui migrent vers le cloud, des utilisateurs qui travaillent à distance, la surface d'attaque augmente aussi vite que ce monde change. Chaque jour le risque augmente un peu plus, pourtant chaque jour, chaque entreprise, chaque nation est un peu plus dépendante de cette transformation digitale accélérée par les pandémies.

La confiance dans le numérique n'est pas un choix, c'est devenu une nécessité. Restaurer chaque jour un peu plus cette confiance, c'est la vision de Palo Alto Networks. Alors face à ces risques, la cybersécurité a toujours été réactive, elle a toujours répondu ponctuellement à un problème.

En quoi consiste son activité ?

Les entreprises adaptent leurs méthodes de fonctionnement à des contextes en perpétuels changements, notamment liés à la digitalisation. Elles utilisent des moyens de communication toujours plus diversifiés, exposant les données, applications et infrastructures à des risques impactant l'ensemble de l'activité de l'entreprise. L'afflux massif de technologies et de données dans le cloud offre aux cybers attaquant de nouvelles opportunités d'exploitation. Les architectures de sécurité doivent donc s'adapter à cette évolution. Les méthodes de détection manuelle ne peuvent pas protéger les Systèmes d'Information des attaques automatisées. Une approche fondée sur une plateforme intégrée qui offre une visibilité complète et automatisée, la prévention est donc nécessaire.

Leader mondial de la cybersécurité, Palo Alto Networks développe des technologies d'avenir qui transforment le quotidien des utilisateurs et des entreprises. Il est le pionnier de l'architecture Zero Trust³ ([voir annexe 3](#)) avec plus d'une décennie d'expérience.

Protéger les modes de vie numériques contre les cyberattaques. Intelligence artificielle, analytique, automatisation, orchestration... ils innovent sur tous les fronts pour aider les entreprises à relever les défis de sécurité les plus sensibles. Palo Alto Networks est le pionnier dans le Pare Feu de nouvelle génération⁴ ([voir annexe 4](#)) qui apporte la visibilité nécessaire à la réduction de la surface d'attaques et permet d'activer plusieurs fonctions

de sécurité avancées en restant prédictible sur les performances. Palo Alto Networks a su faire évoluer cette ligne de produit historique pour bâtir autour d'elle une vraie plateforme de sécurité homogène profitant des avancées technologiques et élargies aux nouveaux besoins et outils de leurs clients.

Cette plateforme intégrée et un écosystème de partenaires en pleine croissance, leur permet d'assurer la sécurité de dizaines de milliers d'entreprises sur le cloud, les réseaux

MON SÉJOUR

- LUNDI
- MARDI
- MERCREDI
- JEUDI
- VENDREDI

Lundi

Le lundi matin, après un appel téléphonique de 30 minutes sur le planning de la semaine dans la voiture, je suis allé à Thales avec mon maître de stage pour aller configurer le nouveau pare-feu de Palo Alto Networks. Nous avons dû passer tous les dispositifs de sécurité puis un certain Fabrice FAUVEL dont la profession est architecte cybersécurité nous a guidé jusque dans une pièce délabrée du sous-sol où le firewall était déballé. L'architecte réseau m'a ensuite proposé d'aller voir le data center de Thales Vélizy où sont regroupés tous ses équipements informatiques. Il faisait très froid avec de nombreux ventilateurs de partout et des dispositifs de sécurité étaient présents afin de protéger la pièce en cas d'incendie ou d'inondation. En retournant dans la pièce, on s'est rendu compte que le switch prévu pour être branché au firewall n'était pas configuré. Nous sommes donc restés jusqu'à midi pour résoudre le problème. C'est à ce moment que j'ai pu apprendre la base d'une attaque informatique, la Kill Chain⁵ ([voir annexe 5](#)).

Ensuite nous sommes allés manger au restaurant avec des représentants de Safran, le client de Palo Alto, là j'ai pu voir la collègue de Damien, Nathalie REGLADE. Ils forment un binôme, chaque binôme est constitué d'un ingénieur orienté vers la technique et d'un autre plutôt commercial dont le but est de montrer les points forts des produits de Palo Alto afin de les distinguer de ceux des concurrents ([voir annexe 6](#)) (organigramme).

L'après-midi, j'ai découvert le bureau de Palo Alto. Les employés m'ont accueilli à bras ouvert, tout le monde s'est présenté et j'ai eu droit à un badge temporaire pour passer les portes sécurisées de la société. Après avoir fait la visite complète de l'étage, Damien m'a présenté l'organisation de l'entreprise à l'aide du tableau tactile de la salle de réunion. J'ai donc pu apprendre que Palo Alto s'articule autour des six départements suivants :

- le commerce, sa mission est de vendre les produits ou services de l'entreprise, à des prospects.
- le marketing, il réfléchit sur ce que les clients veulent et sur la façon de leur vendre les produits ou services de l'entreprise.
- les ressources humaines, elles assure le recrutement et la gestion des salariés qui effectuent le travail.
- la direction, elle assure la gestion globale de la société et définit les grandes orientations stratégiques. Elle s'occupe également d'évaluer l'argent récolté, de payer les factures et de fixer les prix en fonction du coût des matières premières.
- l'IT (Information Technology) qui est elle-même composée du support, son rôle est de répondre aux alertes des clients.
- Recherche et développement, également appelée UNIT 42 : elle permet à la société d'innover et d'améliorer son offre.

Enfin, j'ai pris connaissance des différentes manières de vendre un produit quelle qu'en soit la nature. Cela peut passer par un grossiste, un intégrateur ou même vendu directement au client.

Mardi

Le mardi matin, le bureau était plein. Compte tenu du protocole sanitaire, un seul bureau sur deux peut être occupé. J'ai donc eu pour tâche de réaliser un atelier sur le pare-feu de nouvelle génération sur CloudShare, un fournisseur de Cloud computing. La plateforme est conçue pour aider les éditeurs de logiciels à réaliser des démos, des PoC (proof of concept, démonstration de faisabilité). Cependant en cybersécurité, le sens du terme preuve de concept n'est pas le même. Dans cette situation, il ne doit pas prouver la faisabilité d'un projet mais démontrer une faille de sécurité dans un système) et des formations complexes, en reproduisant les expériences du monde concret. L'atelier dure 4 heures, l'objectif était de me familiariser avec les différentes plateformes telles que Panorama à l'aide de machines virtuelles. Un document téléchargeable connexe servait de guide, il contenait toutes les étapes nécessaires pour parvenir à configurer un pare-feu.

Lorsque le soleil fut au zénith, pour la deuxième fois de suite, nous sommes allés déjeuner au même restaurant que lundi en compagnie d'un employé de Safran et d'un CSO de Palo Alto. Après une interminable conversation sur l'avancé d'un projet, j'ai pu mettre à l'emploi mes questions préalablement préparées pour interroger Raphaël MARICHEZ, un CSO (Chief Security Officer) de Palo Alto dont le métier sera présenté dans le chapitre suivant.

Vers 14h30, on ne pouvait toujours pas rejoindre le bureau. J'ai donc été attelé à une activité de filtrage URL⁷ ([voir annexe 7](#)) de mon propre ordinateur car la plateforme de sécurité de l'entreprise signalait un spyware tournant sur celui-ci. Un spyware, ou logiciel espion est une famille de logiciels malveillants clandestins qui infectent des applications pour dérober différents types d'informations. Cela consistait à sélectionner des types spécifiques de sites web à bloquer. Avec l'option « personnaliser », on pouvait bloquer une catégorie de page web à une période précise de la journée.

Ensuite, j'ai appris la procédure à suivre pour vérifier la dangerosité d'un malware en général. Lorsqu'on consulte la liste des sites web qu'utilise l'ordinateur sans que l'utilisateur ait fait quoique ce soit, il se peut que vous tombiez sur des URL surprenants et donc suspicieux. Dans ce cas nous avons utilisé Virus total, un site web gratuit qui analyse seulement des fichiers individuels à la demande. Il ne fournit pas de protection permanente pour le système d'exploitation de l'utilisateur. Il faut tout de même rester prudent car les résultats obtenus ne garantissent pas qu'un fichier soit sans danger. Sinon vous pouvez directement taper l'url dans la barre de recherche et non la barre d'url car vous risquez d'ouvrir la page soupçonneuse. Dans le cas d'un malware déjà connu il se peut que vous tombiez sur des résultats expliquant le comportement du logiciel malveillant et dans certains cas rares comment l'éradiquer. La dernière méthode se réduit à analyser les résultats de Panorama afin de déterminer si le cas est critique.

Enfin, j'ai effectué quelques modifications à mes questions pour l'entrevue du lendemain. J'ai fini la journée en commençant à rédiger le plan du rapport et la présentation de l'entreprise.

Mercredi

Le mercredi matin, Damien avait réservé une place au bureau pour que l'on puisse s'y installer.

Dans un premier temps, nous sommes retournés à Thales pour paramétriser le switch et le firewall. J'ai pu moi-même manipuler Panorama pour programmer le switch.

Une fois que vous avez la configuration en place, vous pouvez vraiment commencer à créer vos politiques de sécurité. Les politiques de sécurité sont essentiellement vos règles de pare-feu en tant que telles qui autorisent ou interdisent le trafic d'une source vers une destination. Cependant, l'une des grandes capacités du pare-feu de Palo Alto est de pouvoir filtrer le trafic en fonction de l' ID de l'application. Cela vous permet de filtrer le trafic en fonction de « l'app ID » et non en fonction des règles d'adresse IP et de port. Ainsi, par exemple, vous pouvez simplement autoriser "facebook" et ne pas vous soucier des adresses IP et des ports qui doivent être autorisés. Le Palo est capable de voir l'ID de l'application et de bloquer ou d'autoriser le trafic au niveau de la couche d'application.

Nous nous sommes arrêtés après avoir essayé de récupérer les licences. Une fois installées, elles déverrouillent les différentes fonctionnalités du pare-feu lui-même, notamment la prévention des menaces, le filtrage d'URL... Cependant, l'employé de Thales ne les avaient pas à disposition. Il était l'heure de déjeuner.

Après manger, j'ai découvert l'A.N.S.S.I.⁸ ([voir annexe 8](#)) (agence nationale de sécurité des systèmes d'information) et son site web car l'un des arguments de la collègue de mon maître de stage pour vendre les produits Palo était la certification des produits par l'ANSSI.

Ensuite, j'ai eu pour tâche de réinitialiser un PA-220, l'un des plus petits pare-feux Palo Alto, sans connaître le mot de passe. Pendant les heures qui ont suivi, j'ai recherché sur Internet comment réinitialiser un pare-feu Palo Alto Networks et avec quel logiciel. C'est ainsi que j'ai téléchargé « PuTTY », un programme permettant de se connecter à distance à des serveurs en utilisant différents protocoles. La fenêtre de commandes est personnalisable afin de convenir à tous les utilisateurs.

Il y a tout une procédure à effectuer et quelques mots de code à écrire afin de parvenir au menu de maintenance où il faut chercher la commande qui permet de mettre la machine en mode usine tout en étant branché à celle-ci à l'aide d'un câble Ethernet.

Après quelques minutes d'attente, le PA-220 s'est rallumé avec tous les réglages par défaut, il était comme neuf.

Après avoir fini ma tâche je suis allé dans une salle de réunion avec un collègue de mon maître de stage pour qu'il me présente son métier de chef de projet. Cela a duré plus de temps que prévu car il a tout passé en revue : du besoin que satisfait la société jusqu'à la mise en œuvre (aider le client à utiliser le produit) en passant par la création d'un produit tout en me présentant les études qu'il a effectuées pour en arriver là. Encore merci à lui pour m'avoir expliqué tout cela dans le détail.

Jeudi

Le jeudi matin, mon maître de stage m'a confié la mission de changer le mot de passe du pare-feu réinitialisé car celui qui était utilisé à ce moment était similaire au nom d'utilisateur. J'ai pu apprendre que sans passerelle/gateway les terminaux ne pouvaient communiquer s'ils ne faisaient pas partie du même réseau sachant que dans une adresse IPv4 (constituée donc de quatre octets) :

- de classe A, le réseau est défini par le premier octet (un octet = un chiffre entre 0 et 254).
- de classe B, le réseau est défini par les deux premiers octets.
- de classe C, le réseau est défini par les trois premiers octets.

Il fallait donc faire correspondre les deux premiers octets des adresses IP de mon ordinateur et du firewall pour qu'ils puissent communiquer et donc que j'ai possibilité de changer le mot de passe du pare-feu. L'adresse IP par défaut d'un firewall Palo Alto est 192.168.1.1, j'ai donc changé l'adresse IP de mon terminal en 192.168._._ pour qu'ils fassent partie du même réseau. J'ai donc pu changer le mot de passe.

Après cela, mon maître de stage m'a donné un autre « Lab » à effectuer sur CloudShare. Celui-ci était beaucoup plus compliqué que le précédent, il consistait à prendre le contrôle d'un terminal mais toujours dans le monde virtuel du cloud bien sûr.

Ensuite, la mission qui m'a été attribuée se résumait à refaire la manipulation de mercredi avec un PA-850, un pare-feu étant environ quatre fois plus performant que le PA-220.

Je me suis donc installé dans une salle de conférence pour que le bruit des ventilateurs ne dérangent pas mais il était l'heure de manger. Le supérieur direct de mon maître de stage nous a invité à déjeuner en compagnie de Charlène MIRIANI pour répondre à mes interrogations sur l'avant-vente et je les en remercie.

Suite au repas de midi, j'ai continué les opérations nécessaires à la réinitialisation du firewall puis j'ai changé le mot de passe tout en prenant soin de vérifier au préalable la compatibilité des adresses IP de mon PC et du pare-feu.

La suite de l'après-midi a été principalement consacrée à des entretiens consécutifs avec des employés de Palo Alto :

J'ai eu une entrevue en visio-conférence avec Mélinda Costa, Assistante de direction des principaux managers de France, dont le poste sera plus précisément abordé dans le chapitre suivant.

Puis j'ai eu affaire à la réceptionniste qui a examiné de fond en comble tous les recoins de sa fonction.

Enfin, j'ai eu un troisième entretien de nouveau en visio-conférence, en compagnie de Vincent RIVIÈRE, un ancien collègue de Damien travaillant chez Nutanix, un concurrent. J'ai pu avoir des réponses différentes de celles de mon maître de stage malgré la similitude des deux postes.

Vendredi

Le vendredi matin, je suis allé fixer le PA-850 dans une baie du data center du bureau avec le badge de Damien. J'y suis resté quelques minutes le temps de visser le pare-feu et de comprendre comment il fallait faire car le système de fixation n'est pas le même que ceux qui étaient déjà installés.

Ensuite, j'ai passé le dernier entretien, encore une fois en vidéoconférence avec Thibault PARIS, majors system engineer dont la fonction principale est de répondre aux « breach alert » et d'y remédier.

Le terme Breach alert ou Data Breach désigne l'exposition d'informations confidentielles, sensibles ou protégées à une personne non autorisée. Ces fichiers sont visionnés ou partagés sans permission.

Les fuites peuvent concerner n'importe quel type de données. Il peut s'agir d'informations personnelles, de coordonnées bancaires, de données médicales, ou même de secrets commerciaux ou tout autre type d'informations confidentielles.

N'importe qui peut être victime d'une fuite de données. Ce fléau concerne aussi bien les individus que les entreprises de toute envergure et même les gouvernements.

À l'heure où le numérique connaît un véritable essor et où la société vit la digitalisation en mode accéléré compte tenu de la situation sanitaire, les fuites de données sont de plus en plus nombreuses et engendrent un coût toujours plus élevé. Les entreprises représentent une cible particulièrement attractive de par les nombreuses données à leur disposition.

Une fuite de données peut avoir de lourdes conséquences sur la réputation et les finances d'une entreprise. Lorsque l'incident fait l'objet d'une couverture médiatique, le grand public retiendra que l'organisation a de lourdes lacunes en cybersécurité.

Il deviendra difficile de lui faire confiance, même si elle renforce sa sécurité par la suite. Si des informations confidentielles sont dérobées, et notamment la propriété intellectuelle de l'entreprise, les revenus peuvent être directement impactés.

Pour une organisation gouvernementale, une fuite de données peut exposer les informations à des puissances étrangères. Des informations sur les opérations militaires, les infrastructures nationales ou les dossiers diplomatiques en fuite peuvent compromettre la sécurité du pays.

Pour un individu, le plus grave danger d'une fuite de données est l'usurpation d'identité. Un acteur malveillant peut exploiter le numéro de sécurité sociale ou les coordonnées bancaires de la victime pour se faire passer pour elle.

Pour finir la semaine j'ai commencé le design de mon rapport de stage à l'aide du modèle Word de Palo Alto Networks. Comme Damien a accès au réseau interne de l'entreprise (intranet), il a pu me fournir un document que j'ai pu utiliser pour faire l'en-tête de mon rapport de stage.

J'ai quitté le bureau avec un peu de tristesse. Je serai bien resté là-bas.

DÉCOUVERTE

- PRÉSENTATION DU PRINCIPAL MÉTIER OBSERVÉ
- LES 6 AUTRES PROFESSIONS (INTERVIEWS)

Présentation du principal métier observé

Ses responsabilités et ses qualités

L'ingénieur système est un expert du matériel et des logiciels. Il analyse, optimise et sécurise l'outil informatique de son entreprise afin que tous les utilisateurs disposent d'une installation adaptée et performante. En cas d'incidents complexes, il examine de bout en bout la situation pour effectuer au mieux les réparations qui s'imposent. Il assure une veille technologique permanente afin d'anticiper les évolutions des systèmes.

Cet expert comprend les besoins des utilisateurs, conseille les développeurs, entretient des relations régulières avec les constructeurs, les éditeurs de logiciels, les opérateurs. Il est rigoureux, autonome et fait preuve de méthode. Maîtriser l'anglais et être polyvalent sont des qualités indispensables.

Son rôle

En tant qu'ingénieur système, le rôle premier de Damien est l'écoute du besoin du client afin d'assurer sa fonction de référent. Qu'est-ce qu'il faudrait prendre comme abonnement ?, Quel produit peut satisfaire le besoin du client ?

La seconde étape de la fonction d'ingénieur système est d'éduquer et accompagner le client dans l'installation et la configuration de la solution achetée.

Son expérience et les connaissances requises

- License Bac+3 en informatique des réseaux et sécurité numériques après un Bac S
- Master en cryptographie et intrusion
- Connaissance pratique des produits Palo Alto Networks, en mettant l'accent sur le pare-feu de nouvelle génération et certaines technologies comparatives ; développement technique continu
- Comprendre et présenter efficacement leur plateforme de sécurité à des publics techniques et non techniques
- Solides compétences analytiques pour évaluer des problèmes multivariés complexes et trouver une approche systématique pour obtenir une résolution rapide, souvent sous la contrainte
- Compétences matures et efficaces en gestion du temps
- Expérience et connaissance des menaces réseau modernes et des logiciels malveillants, de l'investigation réseau, des outils et technologies d'automatisation et des technologies de sécurité des terminaux

Salaire

Au niveau du salaire, il varie en fonction de l'entreprise et des années d'expérience. D'après le site www.glassdoor.com le salaire type d'un ingénieur système senior de Palo Alto Networks est de 174 521 dollars américains par an. Si l'on tient compte des primes et des rémunérations supplémentaires, un ingénieur système senior à Palo Alto Networks peut s'attendre à toucher un salaire total moyen de 232 206 dollars américains.

Les 6 autres professions (interviews)

Senior Project Manager – Laurent DUPIN

Le gestionnaire principal de projet (en anglais senior project manager), ou directeur de projet, est chargé de superviser la planification et la mise en œuvre de l'ensemble d'un projet en établissant le budget, en embauchant les membres de l'équipe, en recherchant des fournisseurs et en planifiant le lancement du projet. Ses tâches consistent notamment à fixer des échéances, à fournir des commentaires et à communiquer avec les clients sur l'état d'avancement de leur projet.

Les gestionnaires de projet principaux doivent élaborer un plan d'action pour mener à bien un projet, en travaillant avec tous les services pour s'assurer que leurs besoins et leurs désirs sont pris en compte dans les limites du projet et des restrictions budgétaires.

Les chefs de projet senior peuvent être amenés à exercer les fonctions suivantes :

- Développer des plans de projet qui identifient les besoins en ressources et en budget.
- Organiser des réunions de projet au moins une fois par semaine avec l'équipe et les responsables.
- fournir un retour d'information, des conseils, des mises à jour du projet et des encouragements aux membres de l'équipe
- Gérer les échéances et pousser l'équipe à respecter les délais.

Un projet se déroule en trois temps :

- Création ; le département Recherche & Développement met tout en œuvre pour créer le produit dans les délais demandés. Un suivi est mis en place une fois par semaine pour faire un récapitulatif de ce qui a été fait et ce qu'il reste à faire.
- Vente ; on vend une licence de logiciels tout en conservant les droits d'auteur. C'est un procédé commercial où l'acheteur paie la conclusion d'un contrat de licence avec le producteur d'un logiciel en échange de l'utilisation du logiciel.
- Mise en œuvre ; éduquer le client à utiliser le logiciel ou le produit.

Un chef de projet senior de qualité doit posséder de solides compétences en communication et en gestion. Il doit être capable de suivre les instructions de la direction, de gérer les budgets et les délais et de promouvoir avec succès le travail d'équipe.

Pour mener à bien un projet, il doit posséder d'autres qualités telles que :

Être un leadership, telles que les techniques de motivation et la gestion des conflits.

Connaissance de l'informatique pour les tableurs et les logiciels de traitement de texte.

Des compétences en matière de gestion du temps, notamment en ce qui concerne la gestion du calendrier et la fixation d'objectifs

Une bonne connaissance du travail effectué par chaque membre de l'équipe

CSO (regional chief security officer (South Europe)) – Raphaël MARICHEZ

Les CSO sont généralement responsables des protocoles de sécurité en ligne, de la gestion des risques et de la réponse aux incidents de sécurité.

Le rôle d'un CSO inclut la sécurité globale de l'entreprise, notamment le personnel et les actifs physiques de l'entreprise, ainsi que les informations numériques et physiques.

Le CSO est responsable de l'élaboration de protocoles de sécurité des mots de passe, de la protection des données de l'entreprise et de la réponse aux violations potentielles après qu'elles se soient produites.

Il fait également partie des personnes en charge de la relation client. Elles sont présentes avant, pendant et après l'achat. L'objectif étant d'instaurer une relation de confiance sur le long terme. Elles sont également chargées de répondre aux demandes des clients mais aussi d'interpréter les données afin de mieux comprendre leurs comportements et d'établir une stratégie de fidélisation. Afin d'assurer ce rôle, il est nécessaire de se remettre en question régulièrement.

Pour arriver à ses fins, il a fait un Bac S pour intégrer les grandes écoles d'ingénieurs suivantes : Polytechnique et ensuite Télécom Paris.

Il a 15 ans d'expérience après avoir été le manager d'environ quarante personnes dans une autre entreprise.

Entretien sur les métiers de l'avant-vente – Éric ANTIBI & Charlène MIRIANI

L'ingénieur avant-vente est délégué de fournir une assistance technique aux ingénieurs commerciaux dans le but de les aider lors de la négociation de contrats avec le client et répondre ainsi à ses questions techniques.

Il travaille principalement en binôme avec les ingénieurs commerciaux, mais peut également être amené à collaborer avec les services de recherche et développement (pour analyser un besoin spécifique pour un client par exemple) ou encore les départements marketing et production. Il a donc besoin d'être polyvalent entre les différents départements.

L'ingénieur avant-vente va ensuite accompagner l'ingénieur commercial auprès du client pour l'aider à présenter la réponse à l'appel d'offre et répondre aux questions des clients. Il est en mesure de présenter des arguments d'ordre technique, d'effectuer des démonstrations et des présentations de produits de façon à rassurer le client quant à la pertinence des choix techniques.

L'ingénieur avant-vente doit être à l'aise dans ses relations avec les clients, ainsi qu'en communication aussi bien écrite qu'orale. Il doit être capable de travailler en équipe et collaborer avec différents services internes et prestataires externes. L'écoute est donc tout aussi indispensable que la communication. Il doit pouvoir arrêter un choix technique entre plusieurs solutions et apporter suffisamment d'arguments pour convaincre ses interlocuteurs de la pertinence de l'option retenue. C'est également le rôle d'un ingénieur commercial.

Afin de devenir Ingénieur avant-vente chez Palo Alto, il est nécessaire de faire une école d'ingénieur avec une orientation dans l'informatique.

Assistante de direction – Mélinda COSTA

Le rôle d'Assistante de direction est de gérer les emplois du temps des managers à l'échelle internationale. Son rôle d'assistante de direction est d'assister les managers haut gradés et de soutenir leurs équipes. Elle est aussi là pour simplifier la vie professionnelle quotidienne de ces managers leaders. Sa fonction consiste à planifier et à exécuter des réunions importantes, à établir des ordres du jour, à superviser la logistique des réunions et à assurer le suivi des participants. Planifier et coordonner un calendrier de déplacements internationaux et nationaux, et de voyages d'affaires. Consolider et préparer des informations et des présentations. Faire preuve de discréption et d'intégrité en traitant avec des personnes de très haut niveau, notamment des membres du conseil d'administration, des investisseurs, des dirigeants seniors, des clients et des partenaires, et d'autres organisations. Planifier les événements liés aux projets, les réunions hors site, les budgets et les préparatifs des réunions du conseil d'administration et des hauts dirigeants.

Son second rôle consiste à être un support pour les équipes de ses patrons. Elle doit également répondre aux emails notamment de clients de son patron. Enfin elle doit être organisée et coopérer avec les autres assistantes de direction notamment lors de rendez-vous communs entre leurs patrons, cela lui permet de créer un réseau. Il faut pour accomplir cette tâche en intégralité avoir un esprit d'équipe.

Pour en arriver là, Mélinda a passé un certificat d'aptitude professionnel pour ensuite faire un bac pro. Puis elle a réalisé un Brevet de Technicien Supérieur « assistante de direction » en alternance qui se déroule sur deux ans. Il forme les étudiants à traiter de tâches relatives à l'administration, à la communication ainsi qu'à l'organisation.

Réceptionniste

La réceptionniste est généralement la première personne que les clients rencontrent lorsqu'ils entrent dans votre bureau, il est donc important de faire une bonne première impression. Les clients se sentent à l'aise lorsqu'ils voient des employés de bureau courtois, professionnels et capables de gérer plusieurs tâches avec facilité.

La réceptionniste de Palo Alto Networks France accomplit beaucoup de tâche de nature différente durant la journée telles que :

- Accueillir les clients
- S'occupe de toute demande (accès parking, ordinateur, badge, réservation des salles de réunion, photocopies)
- Elle récupère le courrier ainsi que les factures
- Elles donnent les badges aux nouveaux employés ou toute personne éligible et gère leur place dans le parking
- Lorsqu'un employé part, elle doit s'occuper de récupérer le badge, les ordinateurs et pares-feux empruntés à l'entreprise et les envoient à Amsterdam (c'est la procédure).
- Les qualités requises pour être un réceptionniste qualifié sont : compétences téléphoniques, communication verbale, écoute, professionnalisme, organisation...

Global System Engineer de Nutanix, une société de cloud – Vincent RIVIÈRE

Le Senior System Engineer (SSE) est un professionnel de la vente technique orienté client qui fournit des conseils avant-vente, une orientation technique et une assistance pratique aux clients et aux partenaires de distribution. Le SSE travaille en équipe et collabore avec les équipes commerciales pour recommander et concevoir des solutions efficaces et appropriées pour les clients (écoute et patience), basées sur les offres de son entreprise.

Le SSE agit de manière consultative et est considéré comme un expert dans son domaine par les équipes de vente, les partenaires commerciaux et les clients.

Ses responsabilités sont :

Comprendre les moteurs de l'entreprise du client et comment les adapter à une solution.

Fournir une assistance aux partenaires de distribution sélectionnés sur un territoire défini, comprenant : des mises à jour régulières sur les produits et les solutions, des ateliers personnalisés, un programme d'accompagnement des SE (system engineer), et toute autre tâche nécessaire pour permettre au partenaire de fournir un support indépendant avant la vente pour les opportunités de petite à moyenne taille.

Gérer, surveiller et effectuer des évaluations de solutions et des preuves de concept pour soutenir les opportunités de vente, directement ou par l'intermédiaire de partenaires de distribution.

Fournir des rapports et des commentaires sur les comptes clients et les activités sur le terrain aux ventes, à la gestion des produits et à l'ingénierie.

System Engineer Majors – Thibault PARIS

Comme les autres SE, Thibault travaille avec son partenaire commercial pour établir des relations avec les clients dans le but de les aider à détecter et à prévenir les cyberattaques et les brèches avancées en les conseillant sur les applications à déployer à partir de la plateforme Palo Alto Networks. Les ingénieurs systèmes ont une connaissance technique approfondie des produits de cybersécurité, des intégrations et des cybermenaces critiques auxquelles sont confrontés les environnements de leurs clients potentiels.

Palo Alto a besoin de ces guides techniques pour travailler avec leurs équipes de vente, en fournissant une formation et un support technique. Il établit un climat de confiance avec ses clients et ses équipes, en établissant un rapport solide en tant que conseiller de confiance, et il crée un environnement dans lequel les clients se sentent et sont en sécurité. En outre, il sera appelé à donner son avis à l'équipe de gestion des produits sur les demandes de nouvelles fonctionnalités et les améliorations à apporter aux produits.

La particularité du travail de Thibault, c'est qu'il est également en charge de traiter les Breaches Alerts, plus communément appelées Data Breaches (décris dans le chapitre précédent).

Pour faire ce métier, Thibault a réalisé une licence en sécurité informatique de trois ans en alternance puis il a fait un CEH (Certified Ethical Hacker) certifiant ses compétences en recherche de faiblesses et de vulnérabilités à l'encontre d'un système cible.

IMPRESSIONS

- CE QUE J'IMAGINAIS AVANT LE STAGE ET CE QUE J'AI PU OBSERVER
- EST-CE UNE EXPÉRIENCE INTÉRESSANTE ?
- EST-CE UNE AIDE POUR MON PROJET PROFESSIONNEL ?
- CONCLUSION

Ce que j'imaginais avant le stage et ce que j'ai pu constater

Ce stage m'a permis de voir en réalité un métier dans tous ses angles.

J'ai pu me rendre compte que l'ingénieur système a une facette commerciale étant donné que l'organisation par binôme impose un collègue commercial à chaque ingénieur. Par conséquent, je suis déjà certain de ne pas m'orienter dans la vente.

Avant cela, je pensais qu'on serait avec le chef de projet pour développer de nouvelles technologies de sécurité. J'imaginais l'ingénieur système plutôt proche des développeurs et de l'unité « recherche et développement » également appelée UNIT 42 chez Palo Alto Networks. Unit 42 est l'équipe de renseignement sur les menaces de Palo Alto Networks. Composée de chercheurs chevronnés en cyber sécurité et d'experts du secteur, Unit 42 rassemble, étudie, analyse et fournit des informations sur les dernières menaces, puis les partage avec les clients, partenaires et la communauté Palo Alto Networks pour mieux protéger les entreprises, fournisseurs de services et environnements informatiques gouvernementaux.

Unit 42 détecte également des groupes adversaires en analysant les données collectées à partir de la plateforme de sécurité de Palo Alto Networks pour fournir un contexte aux motivations et aux méthodes d'un attaquant. Ils déterminent quelles données sont nécessaires pour répondre aux questions sur les menaces pesant sur leurs clients. Enfin, ils collectent ces données à partir de sources internes et externes et les exécutent via un processus détaillé d'analyse des menaces.

Unit 42 est entièrement supportée par l'équipe d'ingénierie de Palo Alto Networks, qui offre des années d'expérience dans la détection et la prévention des attaques contre les entreprises.

Je ne pensais également pas que Damien serait dérangé par des appels de collègues ou des mails de clients rencontrant des problèmes avec les produits reçus toutes les cinq minutes. Dès qu'on a du temps libre ou qu'on est dans la voiture pour aller à un rendez-vous avec un client, il faut rappeler les personnes dont on a manqué l'appel ou participer à une visio-conférence sur les stratégies à adopter ou à changer dans la société.

Enfin, j'imaginais que l'ingénieur système travaillait seulement en compagnie du chef de projet et de personne d'autre. Le stage m'a permis de voir les relations qu'il peut avoir et avec quelles personnes au sein de l'entreprise. Ainsi, j'ai pu apprendre qu'il travaillait en coopération avec un commercial, néanmoins, toutes les entreprises n'adoptent pas la structure stratégique qu'est l'organisation par binôme.

Malgré les différences entre ce que j'imaginais et ce que j'ai pu observer, je reste enthousiaste à l'idée de faire ce métier du moins m'orienter dans ce domaine. Tous ses aspects me plaisent hormis la facette commerciale. Je pense pouvoir tout de même trouver un métier similaire qui ne revendique pas de qualités commerciales ni de compétences dans le marketing.

Est-ce une expérience intéressante ?

1. Premier pas dans le monde du travail

Pour commencer, mon stage a été l'opportunité de faire un premier pas dans le monde du travail et de découvrir les codes, la culture et le fonctionnement d'une entreprise en général. Mais plus encore, ce stage m'a permis de découvrir et approfondir mes connaissances dans l'informatique, les systèmes d'information et leur protection. Je suis donc très heureux d'avoir eu l'opportunité de faire mon stage en coordination avec mes centres d'intérêt et mes perspectives de carrière.

2. Bâtir un réseau

Ce stage a été une bonne opportunité pour me construire un carnet d'adresses. A l'avenir, je pourrai me tourner vers ces personnes pour demander conseil, profiter de leur expérience acquise, les choses à faire, à éviter, ou encore comment régler certaines situations. Il m'a permis d'établir des contacts avec le monde de l'entreprise

3. Apprendre auprès de professionnels

Un stage vous autorise à prendre le temps de comprendre les tâches qui vous sont demandées et l'utilisation de nouveaux outils. Le but était d'en apprendre le plus possible auprès de professionnels qui étaient justement là pour me guider. Ce sont les mieux placés pour transmettre leur savoir et leurs conseils. Le stage a constitué une rare occasion d'apprendre tout en ayant quand même des responsabilités.

4. Mettre en pratique mes connaissances acquises en cours

Cela a également été une bonne manière d'appliquer mes connaissances acquises lors des cours au collège à de vrai problématiques d'entreprises. Autrement dit, c'était l'occasion de passer de la théorie au concret . Apprendre est une chose, mais mettre en application mes compétences en est une autre. Cela m'a permis de percevoir les enseignements communiqués à l'école d'un nouvel œil et de découvrir de nouveaux centres d'intérêts. Le stage a été l'occasion de faire un premier pont entre les connaissances acquises et le travail. J'ai pu mettre en pratique ce que j'ai appris mais aussi en apprendre davantage.

5. Développer des compétences et se professionnaliser

Le stage m'a apporté de nouvelles compétences notamment en informatique ou dans le commerce telles que les différentes stratégies d'approche à adopter lors de conversation avec le client. J'ai pu aussi renforcer l'écoute de l'anglais et notamment celui des indiens, très difficile à comprendre.

Enfin, cela vient confirmer mes premières idées de ce que représente une entreprise comment elle est organisée et pourquoi, mes aspirations professionnelles ou au contraire, ce que je ne souhaite pas faire.

Est-ce une aide pour mon projet professionnel ?

Au cours de ce stage, j'ai beaucoup appris. Les apports que j'ai tirés de cette expérience professionnelle peuvent être regroupés autour de trois idées principales : les compétences acquises, les difficultés rencontrées, les choses à améliorer pour faire ce métier.

Par exemple, au cours des différents entretiens que j'ai pu avoir, la majorité des fonctionnaires ont répondu que la qualité la plus importante était l'écoute :

« L'écoute du client permet d'identifier tous les besoins et attentes des clients pour les évaluer et bâtir une offre conséquente de l'entreprise. C'est un préalable précieux pour définir les spécifications des produits ou services qu'on leur destine et ne pas s'en écarter. »

Seulement, pour moi, c'est une qualité que je dois renforcer car ce concentrer plusieurs heures sur un écran dans le but de configurer un pare-feu me paraît encore compliqué.

Le stage m'a permis d'avoir un premier contact avec le monde de l'entreprise et du travail. J'ai pu y découvrir un secteur d'activité, des métiers, mais aussi le fonctionnement d'une entreprise et les différentes règles à respecter en milieu professionnel. Ce stage a été bonne occasion pour confirmer mes envies à propos de mes aspirations professionnelles. Il m'a tout de même permis de préciser les différentes fonctions (rôles, qualités, conditions de travail...) d'une entreprise dont l'activité économique est orientée vers la protection des systèmes d'information.

Ce stage fut tout à fait enrichissant pour moi car il m'a permis de découvrir le domaine de la cybersécurité, ses acteurs, ses contraintes, mais aussi de participer concrètement à ses enjeux au travers de mes missions.

Aujourd'hui, cette expérience vient confirmer le fait que j'ai fait le bon choix d'orientation et me permet d'affiner mon futur projet professionnel. En effet, je sais désormais que configurer un firewall, rechercher les virus - pour que chaque jour le monde soit un peu plus sécurisé que le précédent – sont des tâches qui me sont tout à fait adaptées, d'ailleurs ces missions pourraient constituer ma future spécialité.

En revanche, je sais aussi que je ne suis pas fait pour assurer les relations entre le client et l'entreprise car on ne sait jamais qui sera notre interlocuteur...

Comme je l'avais prévu et le stage vient confirmer cette idée, je m'orienterai vers un bac général à orientation scientifique. Probablement que les spécialités seront : physique-chimie, sciences de la vie et de la terre ainsi que sciences de l'ingénieur équipées d'une option en mathématiques expertes.

Avec ce bac je pourrais espérer intégrer une classe préparatoire scientifique pour aboutir dans une école d'ingénieur ou d'informatique.

Conclusion

Notre corps écoute, crie et se souvient. Bactéries, algues, champignons, plantes et animaux signalent, de même, leur présence et perçoivent l'environnement, chacun à sa façon; sans des échanges d'énergie, certes, mais d'information aussi, nul organisme ne survivrait. Avant de se faire humaine, la communication caractérise le vivant comme système ouvert : les cellules communiquent entre elles dans les corps autant que ceux-ci entre eux parmi leur niche écologique. A petite échelle, les réactions chimiques, et dans les grandes, les orages et les galaxies, échangent encore de l'énergie et de l'information, au sein de la matière inerte.

Or, nous autres, hommes, ajoutâmes à ces performances, purement physiologiques ou physiques, une panoplie d'artefacts destinés à relayer notre corps dans ses activités de communication; cet arsenal de messageries et de sémaphores varia au cours de l'histoire. Tout récemment, les technologies électroniques bouleversèrent encore l'ensemble des outils permettant de recevoir l'information, de la stocker ou de la conserver, de l'émettre ou de la transmettre.

Nous avons connu au moins deux bouleversements du même genre dans toute l'histoire: l'invention de l'écriture et celle de l'imprimerie. Gravée sur la pierre, le bronze ou des tablettes de cire, avant qu'on puisse la lire sur papyrus ou papier, la première contribua, de manière décisive, à créer les premières villes, dans le Croissant fertile, de grands Etats organisés sous les règles d'un droit écrit - code d'Hammourabi, loi mosaïque - , assouplit et accéléra les échanges commerciaux grâce à la frappe des monnaies, donna leur essor aux sciences et à la pédagogie, en Grèce ancienne, ainsi qu'aux religions monothéistes, que l'on peut définir, justement, comme des cultes de l'Ecriture. Mieux encore, nous partageons, aujourd'hui, le temps humain, en deux parties distinctes, la préhistoire et l'histoire, celle-ci commençant, précisément, dès l'apparition des premiers textes gravés.

Or dès qu'à la Renaissance apparaît l'imprimerie, les banques italiennes transforment les échanges commerciaux en Méditerranée, ou les lettres de change remplacent la monnaie; elles lancent, du coup, le premier capitalisme; la circulation des livres favorise l'indépendance individuelle prônée par la Réforme protestante, donc la démocratie politique et le droit civil.

L'information est la matière première la plus précieuse pour la compétitivité des entreprises au XXI^e siècle et l'intelligence – humaine ou artificielle – a besoin de cette connaissance pour aider à la prise de décision. Le partage de données et la diffusion de connaissances sont donc les domaines les plus sollicités de l'informatique dans tous les domaines d'activité, de la grande distribution à la recherche médicale. Les systèmes d'information ont permis, à partir des années 1970, d'optimiser les activités de production de l'entreprise, ils ont aussi permis d'engranger dans les bases de données de véritables « gisements » d'informations. L'idée s'est alors faite dès les années 1980, de les utiliser à des fins décisionnelles et de les organiser pour en extraire de précieux renseignements.

Les exigences de la sécurité de l'information au sein des organisations ont conduit à deux changements majeurs au cours des dernières décennies. Avant l'usage généralisé d'équipements informatiques, la sécurité de l'information était assurée par des moyens physiques (classeurs fermés par un cadenas) ou administratifs.

Avec l'introduction de l'ordinateur, le besoin d'outils automatisés pour protéger fichiers et autres informations stockées est devenu évident. Ce besoin est accentué pour un système accessible via un téléphone public ou un réseau de données. On donne à cette collection d'outils conçus pour protéger des données et contrecarrer les pirates le nom de sécurité informatique.

Vous l'aurez compris, la sécurité numérique représente un enjeu économique de taille pour les entreprises et leurs dirigeants. Le nombre d'offres d'emploi a presque quadruplé dans le secteur de la sécurité informatique. Les entreprises sont donc prêtes à investir fortement, notamment en ressources humaines, pour réduire les coûts des cyberattaques. La cybersécurité est au cœur des priorités de tous : Etats, entreprises, particuliers. La transformation numérique cyber sécurisée et durable s'avère donc définitivement une histoire collective. Alors agissons ensemble pour bâtir un monde numérique au service du progrès de l'humanité.

Par conséquent, c'est ce qu'a commencé l'Agence nationale de sécurité des systèmes d'information. L'ANSSI instruit et prépare les décisions gouvernementales relatives à la sécurité du numérique et à celle des données sensibles. Elle participe également à la construction et à la maintenance des réseaux et des terminaux sécurisés pour les services de l'État. L'agence accompagne ainsi les cabinets du président de la République, du Premier ministre et des membres du Gouvernement dans la sécurisation de leurs systèmes d'information.

Je tire un bilan très positif de ce stage, qui fut une expérience très enrichissante tant sur le plan professionnel que personnel. Sur le plan professionnel d'abord, j'ai pu appréhender toutes les facettes des métiers d'une entreprise du numérique. Sur le plan personnel ensuite, j'ai pu comprendre que le domaine de la vente ne représentait pas ce qui me correspondait le plus. Au cours de cette période, comme dans toute phase d'apprentissage, il m'est par ailleurs arrivé de faire quelques erreurs.

“ Ayons La Vision d'un Monde Où Chaque Jour Est Plus Sûr Et Plus Sécurisé Que Le Précédent. ”

Palo Alto Networks

“ L'Homme Et Sa Sécurité Doivent Constituer La Première Préoccupation De Toute Aventure Technologique. ”

Albert Einstein

ANNEXES

- CHIFFRES ET INFORMATIONS SUR L'ENTREPRISE
- SERVICES DE PALO ALTO EN IMAGE
- ZERO TRUST
- TOUT SUR LE PARE-FEU
- KILL CHAIN
- ORGANIGRAMME
- FILTRAGE URL
- ANSSI (AGENCE NATIONALE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION)

Annexe1 Chiffres et informations sur l' entreprise

Date de création de la Société	2005
Origine de la société	USA
Forme juridique	Société de droit étranger
Première commercialisation en France	2009
Chiffre d'affaire global année fiscale 2020	4,3 milliards de dollars
Chiffre d'affaire France année fiscale 2020	107 millions de dollars
Nombre de clients	+75 000 clients dans 150 pays
Nombre de clients en France	+4 000 clients
Effectifs globaux année fiscale 2020	+8 000 personnes
Effectifs France année fiscale 2020	+100 personnes

Plus de 65 000 clients dans plus de 150 pays travaillant dans de nombreux secteurs.

- Plus de 85 % des sociétés du Fortune 100 et plus de 63 % des entreprises du Global 2000 leur font confiance pour améliorer leur approche en matière de cybersécurité.
- Le chiffre d'affaires pour l'exercice 2019 a atteint 2,9 milliards USD, soit une croissance de 28 % par rapport à l'année 2018.
- Classement, pour la septième année consécutive, parmi les leaders du Magic Quadrant de Gartner consacré aux pares-feux réseau.
- Partenariats avec des leaders de renom tels qu'Accenture, Alibaba, Amazon Web Services, Microsoft, Proofpoint, PwC, Splunk, Tanium et VMware.
- Organisation implantée mondialement (zones Amériques, EMEA, Asie et Japon) et reconnue pour ses services exceptionnels, avec notamment :
 - Un service d'assistance désigné comme « service client exceptionnel » par J.D. Power et TSIA (en 2015, 2016, 2017 et 2018).
 - Un engagement dans l'assistance clientèle récompensé par l'évaluation « Excellent mondialement » de la part de TSIA (en 2015, 2016, 2017 et 2018).
- Introduction en bourse en juillet 2012 ; symbole boursier du NYSE : PANW.

Annexe 2 : Les services en image



Le Zero Trust est une stratégie de sécurité informatique créée à l'origine par l'analyste de Palo Alto Network, John Kindervag. Il est rapidement adopté par un nombre croissant d'entreprises. Cette stratégie est basée sur le principe de la confiance zéro.

Les menaces pouvant affecter le système d'information augmentent considérablement. En parallèle, les usages changent, notamment avec le télétravail et le stockage des données des entreprises en ligne. Destiné à diminuer les risques divers, le Zero Trust considère que les acteurs internes et tous les réseaux sont sources potentielles d'actes malveillants en plus des menaces extérieures. Cela implique qu'aucune confiance ne doit être accordée aux activités sur les réseaux de l'entreprise ni aux acteurs, même s'il s'agit de collaborateurs. Une approche Zero Trust inclut notamment la gestion des identités en plus de la protection réseau.

Même si un utilisateur est digne de confiance, son accès peut constituer une

Annexe 3 : Zero Trust

Ste

Annexe 4 : Pare-feu

source accidentelle de menaces, en particulier lorsqu'il se connecte depuis un terminal infecté. Pour y remédier, le Zero Trust préconise l'interdiction d'accès en cas de faille au niveau de l'équipement.

Le pare-feu est une passerelle filtrante qui protège un ordinateur ou un réseau des intrusions provenant de sources externes (comme Internet). Il filtre en effet les paquets de données qui sont échangés. Il est parfois traduit comme coupe-feu, barrière de sécurité ou garde-barrière.

Les firewalls nouvelle génération combinent la technologie traditionnelle des pares-feux avec des fonctionnalités supplémentaires, telles que l'inspection du trafic crypté, une inspection approfondie des paquets. Les firewalls de base n'examinent que les en-têtes de paquets, l'inspection approfondie examine les données contenues dans le paquet, ce qui permet aux utilisateurs d'identifier et d'arrêter plus facilement les paquets de données malveillantes.

Néanmoins, afin de filtrer les paquets de données encapsulés, il a besoin de se baser sur un ensemble de règles de sécurité c'est pourquoi il est nécessaire de le configurer avec soin pour lui donner un maximum d'efficacité. C'est la raison pour laquelle il est préférable de faire appel à un professionnel.



Source de l'infographie :

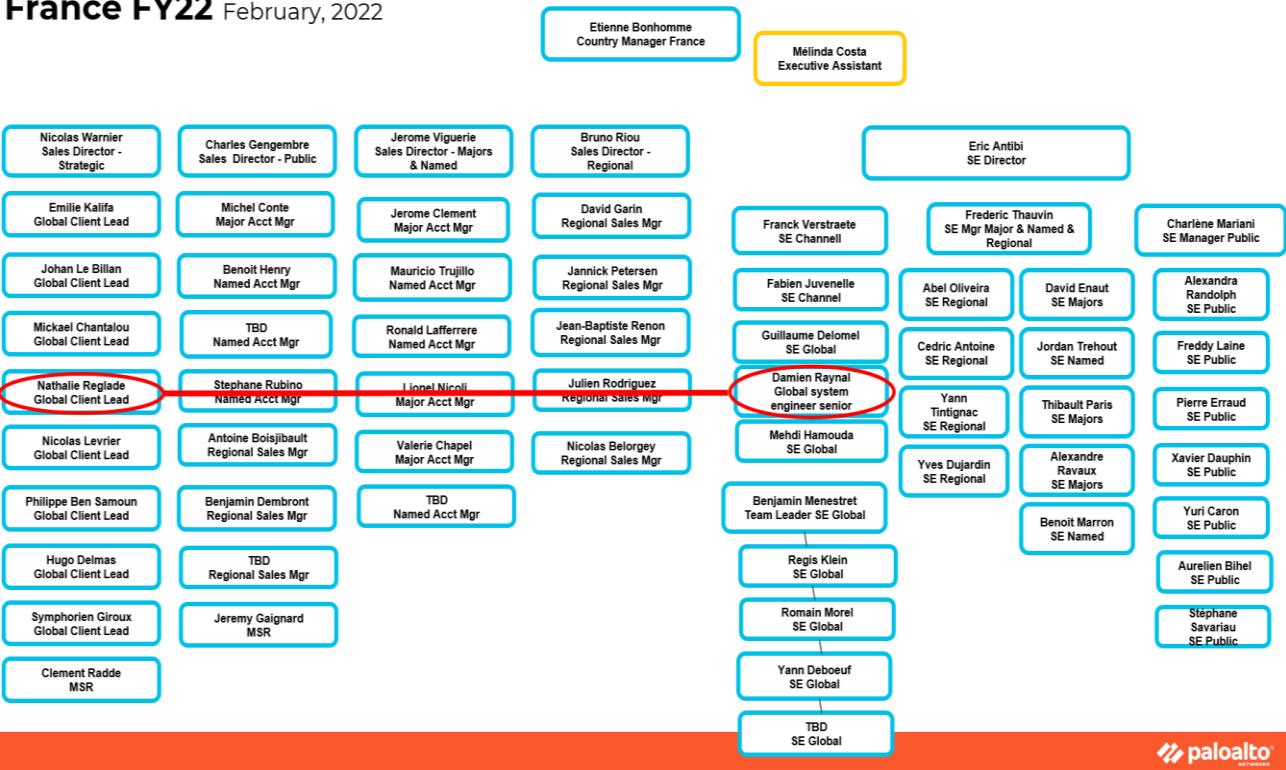
<https://www.manika-consulting.com/infographie-la-cyber-kill-chain-en-7-etapes/>

La Chaîne d'intrusion décrit les phases d'une cyberattaque, de la reconnaissance à l'exfiltration de données. Celle-ci peut également être utilisée comme outil de gestion, afin d'améliorer en permanence la défense du réseau. La chaîne cybercriminelle aide à comprendre et combattre les ransomwares. Depuis sa création, la chaîne cybercriminelle a évolué pour mieux anticiper et reconnaître les menaces internes, les ransomwares avancés et les attaques innovantes.

Annexe 5 : La Kill Chain

Annexe 6 : organigramme

France FY22 February, 2022



Les utilisateurs passent de plus en plus de temps sur le Web, surfant sur leurs sites préférés, cliquant sur des liens de courrier électronique ou utilisant une variété d'applications SaaS basées sur le Web, tant pour un usage personnel que professionnel. Bien qu'incroyablement utile pour améliorer la productivité de l'entreprise, ce type d'activité web sans entrave expose les organisations à une série de risques pour la sécurité et l'activité, tels que la propagation des menaces, la perte éventuelle de données.

La technologie de filtrage des URL compare tout le trafic Web à une base de données de filtrage des URL, autorisant ou refusant l'accès en fonction des informations qu'elle contient. Chaque site Web défini dans la base de données est affecté à une catégorie d'URL, ou groupe.

Il Bloque ou autorise le trafic en fonction de la catégorie d'URL, créé un profil de filtrage des URL qui spécifie une action pour chaque catégorie d'URL et attache le profil à une politique. Cela inclut les catégories pour les sites de logiciels malveillants ou de phishing (hameçonnage).

Le phishing est une cyber-attaque dans laquelle une ou plusieurs cibles sont contactées par courrier électronique, téléphone ou message texte par une personne se présentant comme une institution légitime afin d'inciter les individus à fournir des données sensibles telles que des informations d'identification personnelle, des détails bancaires et de carte de crédit, et des mots de passe.

Ces informations sont ensuite utilisées pour accéder à des comptes importants et peuvent entraîner un vol d'identité et des pertes financières.

Annexe 7 : Filtrage URL

Annexe 8 : L'ANSSI

Créée en 2009, l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) est l'autorité nationale en matière de cybersécurité. Placée sous l'autorité du Premier ministre et rattaché au secrétaire général de la défense et de la sécurité nationale, elle bénéficie d'un positionnement lui permettant de déployer une politique globale de cybersécurité et d'en assurer la coordination à l'échelle interministérielle.

La mission première de l'ANSSI est d'assurer par différents moyens la sécurité des infrastructures numériques publiques et privées les plus critiques et de les défendre en cas d'attaque informatique.

Au-delà de ces organisations les plus sensibles, elle s'adresse également à l'ensemble des acteurs de la transformation numérique du pays pour éléver le niveau de cybersécurité global de la nation et favorise les conditions d'un dialogue de confiance avec ses partenaires français, européens et internationaux.

Bibliographie

- Journal "solutions numériques" – Les Défis du travail hybride – 2021
- Guide de la cybersécurité 5eme édition 2021-2022
- <https://www.ssi.gouv.fr/> | site de l'ANSSI
- <https://www.onisep.fr/>
- <https://www.paloaltonetworks.com/>
- <https://www.youtube.com/watch?v=ZCBB0QEmT5g> | Discours de Michel Serres sur les nouvelles technologies : révolution culturelle et cognitive.
- Journaux "Okapi":
 - N°1085 - 10 inventions qui vont changer nos vies
 - N°1101 – Le mystère des codes secrets
 - N°1007 – Les 8 promesses du monde virtuel
 - N°1125 – voyages dans les villes du futur
- <https://www.geekjunior.fr/vocageek-7-un-psywae-cest-quoi-46311/> | publié par Solène Kutzner le 30/12/2021
- <https://fiches-pratiques.silicon.fr/Thematique/cybersecurite-1338/FichePratique/Zero-Trust-qu-est-ce-que-c-est-365817.htm> | Publié le 19/10/21
- <https://www.forcepoint.com/fr/cyber-edu/firewall> | Qu'est-ce qu'un firewall ?
- <https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/what-is-zero-trust.html> | What is Zero Trust Security ?
- <https://www.linkedin.com/>

La sécurité des systèmes d'information est captivante, d'une large richesse scientifique, unissant de nombreuses disciplines, et au contact d'une grande variété d'organisations et d'acteurs, du secteur public comme du monde de l'entreprise, en France comme à l'international.

Elle est aussi un sujet qui bouscule des habitudes politiques, diplomatiques, économiques ou militaires. Considérée par la France comme priorité nationale, la sécurité des systèmes d'information, ou cybersécurité, concerne désormais aussi chacun d'entre nous.

Les formidables applications que permet le numérique ne seront durables que si elles recueillent la confiance de leurs utilisateurs. Pour construire une société capable de faire face à des risques croissants, à des acteurs agiles aux techniques d'attaques de plus en plus élaborées, il faut systématiquement intégrer les composantes de la sécurité numérique.