Rapport de Stage

Conseil Départemental de l'Essonne

William Pascaloaie

Bachelor 1 – Ethical Hacking (EFREI Paris)

Du 2 mai au 30 juin 2025

Table des matières

Remerciements

Je prends un moment ici avant de débuter mon rapport de stage pour remercier toutes les personnes qui ont fait de mon stage une expérience des plus intéressantes et enrichissantes pour moi autant sur le plan professionnel que personnel.

Merci à Lucile FEDERICI qui a été ma tutrice pour ce stage. Je la remercie pour sa disponibilité, sa pédagogie, et surtout sa confiance. Elle a su me laisser de l'autonomie dès qu'elle a vu que je pouvais « gérer » des situations seul, tout en étant toujours là quand j'avais besoin d'aide ou que je devais poser des questions. J'ai beaucoup appris à ses côtés. Je savais que j'avais quelqu'un qui pouvait m'aider et énormément m'apporter, s'ajoute à ça une ambiance des plus paisibles.

Merci à toute l'équipe cybersécurité et au service informatique. J'ai été magnifiquement bien accueilli, ce qui m'a tout de suite mis à l'aise. Même quand tout le monde était occupé, ils prenaient quand même le temps de m'expliquer les choses que je ne comprenais pas. Que ce soient les analystes, les admins systèmes ou les gens du réseau, chacun m'a transmis un bout de son savoir, toujours avec bienveillance, que je garderais précieusement.

Merci aussi à mes professeurs de l'EFREI, car sans les bases vues en cours, je n'aurais pas pu suivre aussi facilement. Ce que j'ai appris à l'école m'a énormément servi pendant ce stage, que ce soient les cours de phishing, réseaux, tout l'apprentissage linux et Windows et puis même le développement web.

Et enfin merci à l'administration et a toutes les équipes de la Direction des systèmes d'information, pour l'accueil, le matériel, l'organisation… Tout était prêt dès mon arrivée, ce qui a vraiment facilité mon intégration. Ce stage m'a permis de découvrir concrètement le quotidien dans un service cybersécurité, et surtout de confirmer que c'est un domaine dans lequel je me vois bien évoluer. J'en ressors avec plus de compétences, plus de confiance, et le sentiment d'avoir vraiment progressé, alors merci à vous.

Introduction

Cette expérience a vraiment marqué un moment clé de ma formation. Étant en première année de Bachelor en Cybersécurité et Ethical Hacking à EFREI Paris, j'ai eu la chance d'effectuer mon stage de première année au sein du service cybersécurité du Conseil Départemental de l'Essonne pendant deux mois. Cette expérience m'a permis d'appliquer différentes connaissances que j'ai eu la chance de voir en cours et de découvrir le fonctionnement d'un service informatique dans une institution publique ainsi que de contribuer à des missions liées à la protection des systèmes informatiques.

Ce rapport a pour but de présenter en détail cette immersion :

- Les différentes missions auxquelles j'ai participé
- Les compétences que j'ai pu acquérir
- Les outils que j'ai appris à utiliser
- Les difficultés rencontrées et les leçons que j'en ai tirées

J'espère que ce rapport plaira à toutes les personnes qui veulent en savoir plus sur la cybersécurité dans le secteur public ainsi qu'à celles qui comme moi sont passionnées par ce domaine.

I. Présentation de la structure d'accueil

1.1 Le Conseil Départemental de l'Essonne

Le Conseil Départemental de l'Essonne est une collectivité territoriale qui prend en charge la gestion et le développement de l'ensemble du département de l'Essonne. Ses missions sont très variées et touchent de nombreux domaines essentiels à la vie quotidienne des habitants.

- **Le domaine social**

  Le Conseil Départemental de l'Essonne joue un rôle crucial dans l'action sociale. Il vient en aide aux personnes âgées ainsi que dans l'accompagnement des personnes en situation de handicap mais aussi dans la protection de l'enfance ainsi que l'insertion sociale et professionnelle des personnes en difficulté.

- **Les routes et les bâtiments**

Il est également responsable de l'entretien et de la modernisation du réseau routier départemental. Cela comprend la rénovation des différentes infrastructures routière comme les ponts, les chaussées ou même les signalisations ainsi que la construction.

- **La culture**

  Le Conseil Départemental soutient la culture sous différentes formes Subventions aux associations culturelles

  - Organisation d'événements
  - Gestion de bibliothèques
  - Les musées et de sites historiques

  Son objectif est de rendre la culture accessible à tous les habitants du territoire car elle est très importante pour chaque personne.

- **La jeunesse**

  Le département met en place des actions spécifiques à destination des jeunes, qu'il s'agisse de soutien aux collèges ou de dispositifs d'aide à la réussite scolaire ou encore d'accompagnement dans la recherche de stages et de formations et d'emplois.

- **L'environnement**

  Le département agit en faveur de la protection de l'environnement, elle agit dans plusieurs de ces domaines tels que :

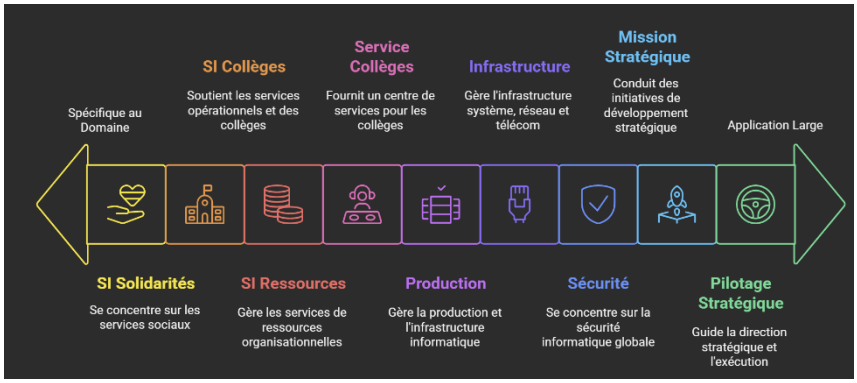
  - La gestion des espaces naturels sensibles
  - Le développement de la biodiversité
  - Les actions pour limiter la pollution et favoriser les énergies renouvelables
  - La gestion durable de l'eau et des déchets.

- **La sécurité**

Enfin, le Conseil Départemental participe à la prévention et à la gestion des risques de sécurité sur son territoire. Cela inclut la sécurité routière, la gestion des plans d'urgence en cas de catastrophe naturelle et le soutien aux forces de sécurité locales par divers moyens logistiques et matériels.

Avec plus de 4 000 employés, cette collectivité utilise un système informatique complexe et sensible qu'il faut absolument protéger contre les risques liés à la cybersécurité qui est un domaine très sensible en ce moment.

1.2 La Direction des Systèmes d'information et le service cybersécurité



La Direction des Systèmes d'information a pour objectif principal de faire fonctionner correctement les équipements numériques tels que les ordinateurs, les serveurs, les réseaux et enfin les applications. Dans ce service il y a une équipe qui est spécialisée en cybersécurité ou MSSI qui travaille à prévenir,

détecter et gérer les problèmes de sécurité. Cette équipe doit créer des règles de sécurité et se doit de surveiller le réseau en permanence. Il gère aussi les incidents et sensibilise les autres agents du département aux bonnes pratiques. C'est dans cette équipe que j'ai pu avoir la chance de réaliser mon stage. Cette équipe est composé actuellement d'un ingénieur de sécurité Senior, d'un Chef de projet sécurité, d'un ingénieur Menace et audit, d'un analyste sécurité et enfin de deux alternants. Je ne pourrais donner aucun nom pour fait de confidentialité.

II. Objectifs et attentes du stage

2.1 Objectifs pédagogiques

Ce stage avait pour but de pouvoir relier les connaissances que j'ai pu recueillir tout au long de l'année de cours avec la réalité qui est en entreprise. L'objectif principal était de me plonger dans le monde professionnel et de voir comment les choses se déroulent directement en entreprise. Plus précisément, je voulais :

- Comprendre comment un service de sécurité informatique est organisé dans une collectivité comme le Conseil Départemental ;
- Découvrir les différentes menaces et attaques que ce type de structure peut subir au quotidien ;
- Participer à la gestion des alertes et des incidents liés à la sécurité ;
- Apprendre à suivre une vraie méthode de travail dans ce domaine ;
- Me familiariser avec des outils utilisés par les professionnels pour surveiller, analyser et réagir face aux problèmes de sécurité.

2.2 Attentes personnelles

En plus des objectifs de stage j'avais aussi des attentes personnelles. Ce stage était important pour moi car il me permettait de mieux connaître le métier vers lequel je me dirige. J'espérais :

- Pouvoir mettre en pratique ce que j'ai appris depuis le début de l'année à EFREI ;
- Comprendre à quoi ressemble vraiment le quotidien dans un service de cybersécurité ;
- Me tester, progresser, et gagner en confiance dans un environnement sérieux ;
- Apprendre à être plus autonome, plus rigoureux, et savoir m'adapter aux situations ;
- Commencer à faire mes premiers contacts dans le monde professionnel, en particulier dans le secteur public, qui m'intéresse beaucoup.

Ce stage était donc pour moi à la fois une première expérience dans mon domaine mais aussi un moyen de confirmer que je suis sur la bonne voie.

III. Intégration et déroulement du stage

3.1 Accueil et immersion progressive

Dès mon arrivée j'ai bénéficié d'un accueil chaleureux et structuré. J'ai, dans un premier temps participé à une visite des locaux, suivis de cela j'ai pu rencontrer tout le personnel qui est dans la Direction des systèmes d'information. Pour donner suite à cela j'ai eu un rappel des règles de sécurité m'ont permis de m'intégrer progressivement dans le nouvel environnement dans lequel j'allais passer mes deux prochains mois. Mon poste de travail a été configuré au préalable par l'équipe SETUP avec un accès limité et sécurisé adapté à mes activités pour que je ne puisse pas toucher à tous les logiciels avec des données trop importantes. Les premiers jours ont été consacrés uniquement à la lecture de la documentation interne (Rappel des règles de sécurité, organigramme de la Direction des systèmes d'information) et à des séances de prise en main des outils (outils phishing, outils lecture de logs etc...) ainsi qu'à des échanges avec les membres de l'équipe pour mieux comprendre leurs missions et leur quotidien.

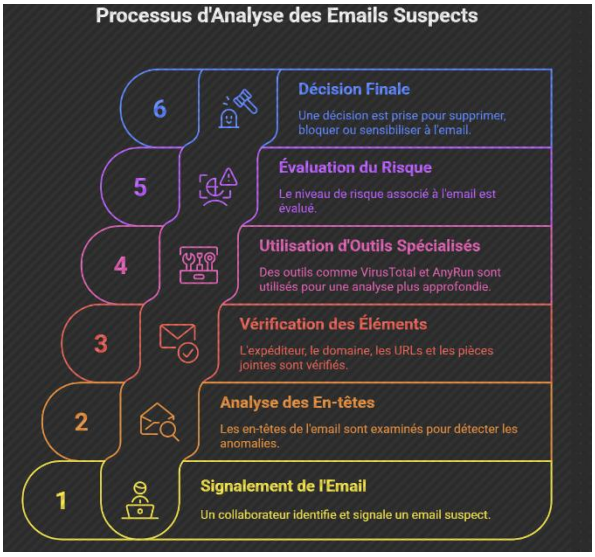
3.2 Accompagnement et autonomie

Tout au long du stage, j'ai été suivi par un tuteur expérimenté qui a su m'encadrer, tout en me laissant progressivement gagner en autonomie. Nous avons mis en place un point hebdomadaire pour faire le bilan de mes activités, poser des questions, et ajuster les objectifs. En parallèle, j'ai été invité à participer à des réunions techniques, des revues de sécurité, et des échanges interservices.

IV. Missions réalisées

Mes missions ont été très variées et représentatives des enjeux actuels de la cybersécurité. Elles ont couvert à la fois des aspects techniques, organisationnels et humains, me permettant d'avoir une vision globale du rôle d'un analyste cybersécurité dans une collectivité territoriale.

4.1 Analyse de courriels suspects (Phishing)



Ma mission principale au sein du service cybersécurité a été d'analyser les courriels suspects signalés par les agents du Conseil Départemental de l'Essonne. Cette mission m'a permis de me confronter aux menaces liées au phishing et à ses variantes, telles que le spear phishing. J'ai acquis une méthodologie rigoureuse en me fiant a toute la procédure crée auparavant par des membres de l'équipe cyber pour examiner en profondeur les e-mails douteux notamment à travers l'analyse des en-têtes, la vérification de l'adresse d'expéditeur, l'observation des noms de domaines utilisés, et le contrôle des pièces jointes ou des liens contenus dans le message.

4.2 Outils utilisés pour l'analyse des e-mails suspects

Pour mener à bien cette mission, j'ai utilisé différents outils qui avaient tous un rôle différent et qui sont gratuit et disponible sur tous les navigateurs. Ces outils m'ont permis de détecter rapidement les tentatives d'hameçonnage et les contenus malveillants :

- VirusTotal : Ce service m'a permis d'analyser les pièces jointes et les liens suspects en les scannant avec une quarantaine de moteurs antivirus. Cet outil m'a énormément aidé à détecter les fichiers exécutables camouflés, les scripts malveillants, ou encore les URLs menant à des sites frauduleux.
- AnyRun : Grâce à cet outil de sandbox dynamique, j'ai pu exécuter des pièces jointes dans un environnement sécurisé pour observer leur comportement en temps réel. Cet outil m'a été très utile pour identifier des payloads ou des tentatives d'installation de malwares.
- FileScan.io : J'ai également utilisé cette plateforme pour obtenir une analyse détaillée des fichiers suspects, avec une vue sur les appels système, les modifications du registre, ou encore les connexions réseau établies par le fichier exécuté.
- MxToolbox : Cet outil m'a été précieux pour analyser les enregistrements DNS et vérifier si les serveurs d'envoi des courriels étaient correctement configurés ou répertoriés comme malveillants. Cela m'a permis d'identifier certains courriels usurpant des domaines légitimes.
- Whois Lookup : J'ai régulièrement utilisé les services de recherche WHOIS pour identifier les propriétaires des noms de domaines utilisés dans les courriels. Lorsque le domaine avait été créé récemment ou qu'il provenait d'un registrar douteux, cela éveillait davantage mes soupçons.
- URLScan.io : Pour examiner plus en détail les liens contenus dans les messages suspects, j'ai eu recours à URLScan. Cet outil nous permet de visualiser le rendu de la page de garde du site qui est visé, d'observer les redirections ainsi que d'obtenir une cartographie des requêtes réseau effectuées par la page.

- Xodo : Pour les documents PDF attachés aux courriels, j'ai utilisé Xodo pour les ouvrir de façon sécurisée et inspecter leur contenu sans risquer d'exécuter de code malveillant intégré.

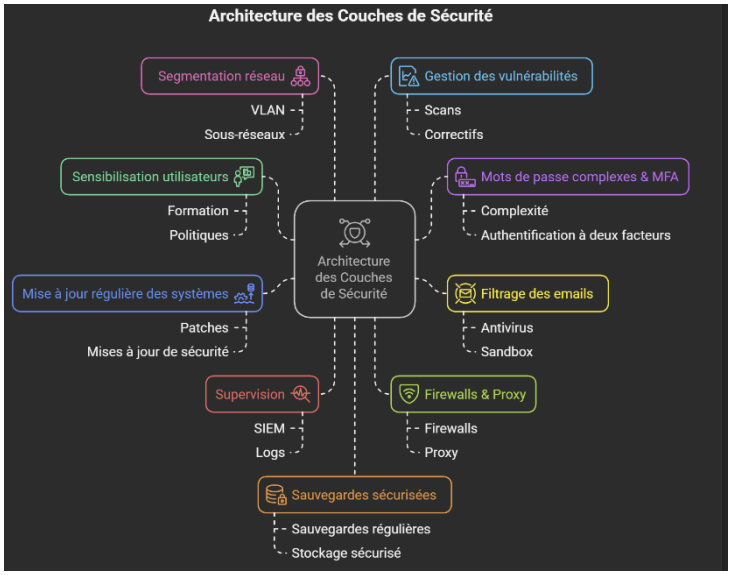
4.2.1 Apport de cette mission

Cette mission de phishing m'a permis de comprendre les différents principes de défense en profondeur dans un environnement réel. J'ai pu observer comment une attaque peut évoluer à partir d'un simple clic sur un lien de phishing et comment il est essentiel de réagir rapidement car il y a d'énorme risque comme les fuites de

Données importantes, ce qui pour un département est assez compliqué à vivre. En parallèle, j'ai pu approfondi mes connaissances sur l'architecture réseau du département, notamment sur les points d'entrée potentiels, les pares-feux, les systèmes de journalisation et les outils de corrélation d'événements. J'ai ainsi pu proposer des mesures concrètes comme :

- La restriction des communications sortantes pour certains postes sensibles ;
- La mise à jour régulière des logiciels de messagerie ;
- Le renforcement des logs de surveillance des e-mails ;
- La sensibilisation continue des utilisateurs face aux courriels suspects.

Pour assurer une protection globale et assez efficace du système d'information, Nous avons besoin d'adopter une approche de défense en profondeur. Cette protection repose sur la superposition de différentes couches de sécurité permettant de réduire les différents risques d'intrusion, de compromission ou bien même de perte de données. Le schéma présente les différentes mesures de sécurité mises en œuvre, organisées par niveaux de protection :



4.3 Étude de vulnérabilités internes

Le service de supervision du département m'a permis de participer à l'analyse de vulnérabilités détectées en interne. Ces alertes concernaient par exemple des postes de travail mal configuré, des services non mis à jour ou des comportements anormaux sur le réseau. Accompagné d'un expert, je participais à la reproduction des conditions d'exploitation de la faille en laboratoire sécurisé. Nous réalisions ensuite une évaluation du risque selon plusieurs critères : accessibilité de la faille, impact potentiel, niveau de privilège requis, et capacité de détection par les outils en place. Cette mission m'a permis de mieux comprendre les principes de défense en profondeur, d'approfondir ma compréhension de l'architecture réseau du département, et de proposer des mesures concrètes comme la restriction de certains accès, la mise à jour de logiciels ou le renforcement des logs de surveillance.

4.4 Actions de sensibilisation et prévention

Conscient que la cybersécurité repose en grande partie sur le facteur humain, j'ai contribué à des actions de sensibilisation à destination des agents du Conseil

Départemental. J'ai notamment assisté à des présentations animées par mes collègues experts en cybersécurité, portant sur les risques suivants :

Risques liés aux clés USB non autorisées

Plusieurs incidents récents démontrent que l'utilisation de clés USB non approuvées sur nos postes de travail représente une menace sérieuse pour l'ensemble de notre système informatique. Ces périphériques non contrôlés présentent trois dangers majeurs :

- Propagation de virus sur l'ensemble du réseau interne
- Installation discrète de logiciels espions ou malveillants
- Point d'entrée potentiel pour des ransomwares (comme l'attaque subie dans le 77)

L'exemple du département de la Seine-et-Marne est particulièrement parlant. Elle s'est déroulée le 6 novembre 2022. Pendant plusieurs mois, les agents de cette collectivité n'ont pas pu accéder à leurs documents professionnels et fournir un service optimal à leurs usagers. Les pirates ont demandé une rançon de 10 millions de dollars. Le département a refusé de payer ce qui a eu pour conséquence la perte définitive de certaines données sensibles.

Sensibilisation aux attaques par hameçonnage

Des exemples concrets ont démontré comment des liens frauduleux, pourtant semblant légitimes, peuvent compromettre des comptes. Ce type d'escroquerie représente une menace constante pour la confidentialité des données.

Sécurité des mots de passe

Nous avons expliqué qu'utiliser le même mot de passe pour plusieurs comptes est risqué. Si un service est piraté, tous vos comptes peuvent être compromis. La solution ? Un gestionnaire de mots de passe. Cet outil :

- Stocke tous vos mots de passe de manière sécurisée
- Génère des combinaisons complexes uniques pour chaque compte
- Reste simple à utiliser au quotidien

Protection des accès à distance

Les connexions externes mal sécurisées sont une cible facile pour les pirates. Nous avons détaillé les bonnes pratiques pour :

- Verrouiller ces points d'entrée sensibles
- Empêcher les intrusions sur le réseau du Département
- Maintenir la sécurité des données même en télétravail

J'ai pu observer comment les experts en cybersécurité adaptent leur discours pour rendre compréhensibles des concepts assez techniques à comprendre. Cette expérience m'a montré l'importance de la pédagogie dans la prévention des risques numériques.

4.5 Utilisation d'outils professionnels

Durant mon stage, j'ai été formé à plusieurs outils essentiels pour les activités du service cybersécurité. Sans pouvoir citer les solutions spécifiques pour des raisons de confidentialité, voici les principales catégories d'outils que j'ai utilisées :

Outils de supervision et monitoring

- **Visualisation des flux réseau** :
  Une plateforme dédiée permettait de surveiller en temps réel l'ensemble du trafic pour détecter des activités suspectes ou des connexions anormales. J'ai appris à identifier des schémas de comportement inhabituels pouvant révéler des tentatives d'intrusion.
- **Centralisation des journaux** :
  Un système unifié agrégeait les logs de sécurité provenant de l'ensemble des équipements (pares-feux, serveurs, stations de travail). Mon rôle consistait à :
  • Analyser les corrélations entre événements
  • Rechercher des indicateurs de compromission
  • Générer des alertes personnalisées
- **Solution de gestion de parc et d'incidents** :
  J'ai utilisé une plateforme complète permettant :
  • Le suivi précis du matériel informatique
  • La gestion des tickets et demandes d'assistance
  • La documentation des configurations
  • La traçabilité des interventions techniques

Cet outil s'est révélé indispensable pour maintenir une vision d'ensemble des actifs et faciliter la résolution des problèmes.

Outils d'analyse et réponse

- **Environnement d'analyse sécurisé** :
  Pour examiner les fichiers suspects (pièces jointes, exécutables) sans risque pour le système d'information.
- **Outil d'investigation rapide** :
  Permettant des analyses préliminaires sur les postes utilisateurs lors d'incidents potentiels.

Outils de reporting

- **Générateur de tableaux de bord** :

  Pour produire des rapports synthétiques à destination de la direction, mettant en évidence les indicateurs clés de sécurité.

L'utilisation de ces différents outils m'a permis de :

1. Comprendre leur complémentarité dans une chaîne de sécurité cohérente
2. Appréhender l'importance d'une bonne intégration entre les solutions
3. Développer une méthodologie rigoureuse d'analyse

Bien que certains outils aient nécessité un temps d'adaptation, l'accompagnement de l'équipe m'a permis de rapidement les maîtriser et d'apprécier leur valeur ajoutée dans les différentes missions qui m'ont été confiées. Cette expérience concrète avec des outils professionnels a considérablement enrichi ma compréhension des infrastructures de sécurité modernes.

V. Compétences développées

5.1 Compétences techniques

Ce stage m'a permis de développer des compétences clés en sécurité informatique :

Détection des tentatives de phishing

J'ai acquis la capacité d'identifier les emails frauduleux en analysant :

- Les incohérences dans l'adresse de l'expéditeur
- Les liens suspects et les pièces jointes inhabituelles
- Les formulations alarmistes ou urgentes
- Les erreurs linguistiques fréquentes
  Cette expertise est cruciale pour prévenir les attaques avant qu'elles ne se produisent.

Analyse des vulnérabilités

J'ai appris à :

- Comprendre et interpréter les bulletins de sécurité (CVE)
- Évaluer la criticité des failles grâce aux scores CVSS
- Adapter les mesures de protection en fonction des risques spécifiques
- Prioriser les correctifs selon l'impact potentiel
- Utilisation d'outils de supervision et de gestion des alertes : J'ai pu interagir avec des outils de sécurité avancés (sans les citer), qui permettent de centraliser, analyser et corréler les événements de sécurité. J'ai appris à filtrer les alertes pertinentes, à repérer les faux positifs et à prioriser les actions à mener.

- Analyse d'emails et de fichiers suspects : En collaboration avec les équipes, j'ai pu effectuer des analyses plus poussées : ouverture de pièces jointes en environnement isolé, décodage d'URL, vérification de hachages, analyse comportementale. Cela m'a permis de comprendre comment les fichiers malveillants sont conçus et diffusés.
- Application de recommandations de sécurité : Après identification d'un risque, j'ai participé à la formulation de recommandations (changement de mot de passe, blocage de domaines, mise à jour de logiciels). J'ai aussi pris part à des réflexions sur la priorisation des actions correctrices dans un cadre institutionnel.

5.2 Compétences humaines et organisationnelles

Au-delà des aspects techniques, ce stage m'a permis d'acquérir des savoir-faire essentiels dans le monde professionnel :

Collaboration en équipe

J'ai appris à m'intégrer efficacement au sein d'une équipe pluridisciplinaire, partager mes connaissances tout en respectant les procédures établies ainsi que d'adapter ma communication selon mes interlocuteurs (collègues, responsables)

Rédaction de documents professionnels

J'ai développé ma capacité à produire des comptes-rendus techniques accessibles à tous, synthétiser des informations complexes et adapter le niveau de détail selon le public cible

Animation de sensibilisation

Mon implication dans la création de supports pédagogiques m'a permis de simplifier des concepts techniques pour les non-spécialistes, concevoir des messages préventifs impactant puis enfin animer des échanges sur les bonnes pratiques

Organisation et rigueur professionnelle

J'ai appris à gérer efficacement mon temps de travail, prioriser les tâches selon leur urgence et importance puis documenter systématiquement mes actions

Approche éthique des technologies

Enfin ce stage m'a sensibilisé aux enjeux de la protection des données personnelles avec l'usage responsable des outils de sécurité et du respect des droits des utilisateurs

VI. Analyse critique de l'expérience

6.1 Retour global sur le stage

Ce stage m'a formé et ouvert les yeux sur la réalité du terrain. Jour après jour j'ai découvert ce que signifie vraiment protéger un système d'information. Il ne s'agit pas seulement de lignes de code ou de pares-feux, mais bien de sécuriser des personnes, des processus et une organisation dans son ensemble pour éviter que celle-ci ne soit inactive ou plus exploitable.

Au cours de cette expérience, j'ai pu concrètement toucher a différents aspects cruciaux de ce secteur. Tout d'abord, la difficulté récurrente de faire comprendre les risques à des non-techniciens. Ensuite l'équilibre délicat à trouver entre sécurité et facilité d'utilisation. J'ai également mesuré l'importance cruciale des petites actions

quotidiennes comme les mises à jour ou la gestion des mots de passe. Enfin, j'ai été frappé par la rapidité avec laquelle les menaces évoluent dans ce domaine.

Plusieurs observations m'ont particulièrement surpris. Notamment le fait que 90% des problèmes rencontrés provenaient du simple fait de négliger des choses simples, et que celles-ci ne sont pas robotiques mais bien humaines. J'ai aussi pu constater que les solutions les plus efficaces étaient souvent les plus simples à mettre en œuvre. J'ai aussi découvert une ambiance de travail particulière qui a été marquée par une urgence permanente mais toujours parfaitement maîtrisée.

Sur le plan personnel ce stage m'a permis d'acquérir des compétences très importantes pour la suite de ma vie. J'ai appris à vulgariser des concepts complexes sans en déformer le sens. J'ai développé une capacité qui est de prioriser les vraies menaces parmi les nombreuses alertes. Le simple fait de regarder tout le temps la documentation afin d'être sûr de ce que je fais est devenue une seconde nature.

Ce qui m'a le plus marqué, c'est d'avoir pu observer comment une équipe qui arrive à être soudée parvient avec des moyens limités à protéger l'ensemble d'un département. Ils ne sont pas forcément nombreux mais très efficaces. Cette expérience a confirmé mon attirance pour ce métier. Non pas pour son aspect technique mais pour son impact concret sur la sécurité de tous.

6.2 Approfondissement de l'analyse de phishing

Dans le cadre de ces analyses, ma démarche incluait systématiquement plusieurs étapes clés : l'examen minutieux des certificats et domaines utilisés, ainsi que des techniques d'obfuscation couramment employées par les attaquants. Je croisais ensuite les signaux détectés avec des bases de données de réputation en ligne. Chaque message se voyait attribuer un score de risque objectif pour faciliter la prise de décision. La comparaison des différentes alertes reçues permettait d'identifier les campagnes de phishing, qu'elles soient ciblées ou massives. Enfin, une remontée automatisée aux systèmes de sécurité garantissait une réponse rapide et coordonnée.

6.3 Entretiens avec la Direction des systèmes d'information et le RSSI

Plusieurs enseignements majeurs se sont dégagés de tous les entretiens que j'ai pu réaliser. Concernant la gestion des priorités, les chefs de projet ont souligné la plus grosse complexité qui est d'arbitrer entre impératifs de sécurité et besoins opérationnels.

Un exemple parlant, ont été les mises à jour des systèmes critiques, où les contraintes de disponibilité entrent fréquemment en conflit avec les recommandations de patching. Au niveau du plan de la collaboration interservices, le RSSI a particulièrement insisté sur l'importance cruciale d'une communication fluide entre équipes. J'ai pu voir concrètement comment les remontées d'alertes étaient gérées en mode projet, avec des réunions de coordination hebdomadaires associant à la fois les équipes techniques et les responsables métiers.

En matière de sensibilisation, les responsables ont noté une évolution positive des mentalités face aux enjeux de sécurité. Cependant, ils ont unanimement pointé la nécessité de renforcer encore les formations pratiques destinées aux utilisateurs finaux.

La méthodologie employée pour ces entretiens a été rigoureuse. Pour chacun des entretiens j'ai procédé à une prise de notes détaillée afin de me rappeler de tout ce qui est dit et que je puisse comparer tout ce qui a été dit par chacun des agents.

Ces discussions ont apporté une valeur considérable à mon stage. Elles m'ont d'abord permis de comprendre les réalités opérationnelles sous-jacentes aux politiques de sécurité. J'ai également développé mon aptitude à mener des interviews techniques pertinentes. Enfin, ces échanges m'ont aidé à identifier des axes d'amélioration pour mes futures analyses de vulnérabilités.

VII. Conclusion et perspectives

J'ai commencé ce stage avec des idées plein la tête, des choses apprises en cours, des films peut-être... La réalité m'a vite rattrapé. La sécurité informatique, ce n'est pas du cinéma. Ce sont des journées à traquer des failles que personne ne voit, à essayer de deviner comment les autres pourraient attaquer, à répéter toujours les mêmes consignes.

J'ai passé des heures à vérifier des logs qui n'en finissent pas, expliquer pour la centième fois pourquoi il faut changer son mot de passe, tester des scénarios d'attaque qui font peur, documenter chaque action comme si c'était vital (parce que ça l'est)

Le déclic a été quand j'ai vu une alerte réelle arriver. Pas un exercice, un vrai danger. L'équipe s'est mise en mouvement, calme mais rapide. J'ai compris ce jour-là que notre travail c'est d'être prêt, toujours. Prêt pour des menaces qui changent tous les jours, prêt à réagir en quelques minutes, prêt à prendre des décisions lourdes.

Ce que j'emporte avec moi sont la sensation d'avoir vraiment protégé quelque chose d'important ainsi que des réflexes que je ne perdrai plus avec aussi la simple habitude de tout remettre en question et enfin des collègues devenus des modèles

Merci à ceux qui m'ont fait confiance, qui m'ont laissé tâtonner parfois, qui m'ont montré sans se lasser. Vous m'avez appris un métier, mais surtout une manière de l'exercer et encore mieux une passion. Je repars différent, et c'est ce qu'il y a de plus précieux.