REPUBLIQUETUNISIENNE

Ministère de l'Enseignement Supérieur

et de la Recherche Scientifique

Université de Gabès

Ecole Nationale d'Ingénieurs de Gabès Département de Génie des Communications & des Réseaux

المدرسة الوطنية للمهندسين بقابس

قسم هندسة الاتصالات والشبكات

RAPPORT DE STAGE OUVRIER

Réalisé par: Siwar Trabelsi

Année Universitaire: 2024/2025

Remerciements

Je tiens à exprimer ma sincère gratitude à toutes les personnes qui m'ont soutenu et accompagné tout au long de mon stage d'observation au sein du département ISM (Information Security Management) d'ODDO BHF.

Tout d'abord, un grand merci à M. Walid, CISO, pour sa vision claire de la sécurité de l'information et pour avoir permis à un jeune stagiaire d'observer le travail stratégique du département. Je tiens également à remercier mes managers, M. Amin Abid et M. Mohamed Nasri, pour leur soutien et leurs précieux conseils tout au long de cette expérience.

Je remercie chaleureusement mes team leaders, M. Mohamed Ali Ellafi et M. Iheb Ben Salem, qui ont été mes encadrants durant ce stage. Leur expertise, leur disponibilité et leur engagement m'ont permis de mieux comprendre les défis quotidiens de la gestion de la sécurité des systèmes d'information. Leur accompagnement et leurs explications ont été essentiels pour enrichir mon apprentissage et approfondir ma compréhension du fonctionnement du SOC (Security Operations Center).

Un grand merci également à toute l'équipe du département ISM pour leur accueil chaleureux, leur disponibilité et pour avoir partagé leurs connaissances et bonnes pratiques de manière bienveillante.

Enfin, je souhaite exprimer ma profonde gratitude envers mes professeurs et encadrants académiques pour leur soutien constant tout au long de mon parcours. Leur enseignement, leurs conseils et leurs encouragements ont été des piliers essentiels dans ma formation et m'ont permis d'aborder ce stage avec confiance.

Merci à tous pour cette expérience professionnelle et humaine inoubliable.

Table des matières

Sommaire

Acronymes

CISO: Chief **I**nformation **S**ecurity **O**fficer

CSIRT: Computer **S**ecurity **I**ncident **R**esponse **T**eams

CTI: Cyber **T**hreat **I**ntelligence

DMARC: Domain-based **M**essage **A**uthentication**, R**eporting, and **C**onformance

DKIM: Domain **K**eys **I**dentified **M**ail

ECP: Exchange **C**ontrol **P**rotection

ISM: Information **S**ecurity **M**anagement

SIEM: Security **I**nformation and **E**vent **M**anagement

SOC: Security **O**peration **C**enter

SPF: Sender **P**olicy **F**ramework

TTPs: Tactics, **T**echniques and **P**rocedures

Listes des figures

Liste des tableaux

Introduction générale

Au cours de mon stage d'observation chez ODDO BHF à Tunis, au sein du département Information Security Management (ISM), j'ai eu l'occasion d'explorer les dynamiques et les processus clés de la cybersécurité au sein de l'entreprise. Oddo BHF, réputé pour son expertise en sécurité des systèmes d'information, dispose d'une équipe de Security Operations Center (SOC) ainsi que d'un Computer Security Incident Response Team (CSIRT) chargé de protéger les données et les infrastructures critiques contre les menaces cybernétiques. Ce stage m'a permis d'observer le fonctionnement administratif du département ISM, ainsi que la répartition des rôles au sein des équipes SOC et CSIRT. J'ai pu observer les différentes équipes présentes, leurs responsabilités spécifiques, et comment elles collaborent pour assurer une surveillance efficace, une détection rapide des incidents et une gestion des risques.

En parallèle de cette observation, j'ai développé un script permettant d'analyser les URL, les hash, les adresses IP et les fichiers, avec les résultats stockés dans une base de données pour offrir une consultation centralisée des analyses. Ce script facilite l'accès aux informations et améliore la gestion des menaces pour les analystes de sécurité. Ce rapport présente un aperçu des connaissances acquises pendant ce stage, en mettant l'accent sur l'organisation des équipes SOC et CSIRT, ainsi que sur l'outil d'analyse que j'ai conçu pour soutenir les opérations de cybersécurité.

Chapitre1

Présentation de l'entreprise et du Département Cybersécurité

I. Introduction

Dans ce premier chapitre, nous allons explorer le cadre dans lequel se déroule ce stage d'observation au sein de l'entreprise ODDO BHF. Ce chapitre a pour but de présenter l'organisation générale de l'entreprise, en mettant particulièrement l'accent sur le département Information Security Management (ISM) et sur le rôle du Security Operations Center (SOC) dans la gestion de la cyber sécurité. Cette présentation permettra de mieux comprendre le contexte dans lequel s'inscrit ce stage et les enjeux liés à la sécurité de l'information au sein de l'entreprise.

II.1 ODDO BHF

Le projet a été réalisé au sein d'ODDO BHF. Nous vous présentons dans une première partie cette entreprise, ses domaines d'expertise et ses implantations. Puis nous exposons son évolution. Enfin, nous vous présentons ODDO BHF Tunis.

II.2 Présentation générale

ODDO BHF est un groupe indépendant de services financiers franco-allemand, créé en 1849 et agréé en tant que banque en 2007. Il est devenu une banque d'investissement et de gestion de capital. Elle est représentée par son associé commandité Monsieur Philippe ODDO.[1]
La société ODDO BHF exerce principalement sept métiers :
1. Gestion d'actifs (ODDO BHF Asset Management - OBAM) : gestion de capital (détenue ou externalisée par un tiers investisseur), gestion de portefeuille (gestion discrétionnaire, gestion conseillée, gestion gérée), gestion de fonds.
2. La Banque Privée (ODDO Private Banking - EBP) : gestion discrétionnaire, gestion conseillée, ingénierie patrimoniale, assurance-crédit et assurance-vie.

3. La banque d'affaires (ODDO Corporate Finance - OCF) : conseil (fusions-acquisitions, ingénierie boursière), marchés de capitaux (actions, dette, notation) et corporate broking (market making et intermédiation).

4. Activités de marché (ODDO Securities), intermédiaire de marché auprès d'une clientèle institutionnelle principalement : analyse financière, analyse crédit, stratégie, analyse économique

et technique, intermédiation actions, intermédiation obligataire, convertibles, futures, roadshows et événements.

5. Tenue de Compte / Rétention de Titres (Services ODDO) : gestion de compte dépositaire, de garde et de valorisation d'OPCVM.

6. Négociation de produits dérivés (Options ODDO) : gestion de marché et intermédiation.

7. Intermédiation des métaux (ODDO Metals).

La Figure1.1 ci-dessous illustre la mise en place de ODDO BHF là où il existe en :

− Six pays en Europe : France, Allemagne, Suisse, Luxembourg, Espagne et Italie.

− Un seul pays en Amérique du Nord : les États-Unis.

− Quatre pays d'Asie : Singapour, le Vietnam, la Chine et les Emirats Arabes Unis.

− Deux pays d'Afrique : Tunis et l'Egypte

FIGURE 1.1 – Localisation de ODDO BHF

II.3 Historique

ODDO BHF est un groupe de services financiers créé en 1849. L'histoire du groupe s'accélère à la fin des années 80 avec l'arrivée en 1987 de Monsieur Philippe ODDO. Les événements qui ont marqué l'histoire du groupe sont :

— 2021 Signature d'un accord de partenariat pour le métier d'intermédiation actions avec Commerzbank en Allemagne

Négociation exclusive avec QUILVEST WEALTH MANAGEMENT pour acquérir 100 % du capital de QUILVEST BANQUE PRIVEE S.A. (QBP)

ODDO BHF renforce son métier de gestion d'actifs avec l'acquisition de METROPOLE Gestion, spécialiste de la Gestion Value

— 2020 Signature des accords de partenariat pour le métier d'intermédiation actions avec ABN AMRO aux Pays-Bas et BBVA en Espagne

Renforcement en Suisse : Acquisition de la plus ancienne banque de Suisse romande, Landolt et Cie, basée à Lausanne et Genève

— 2018 Transfert des activités d'intermédiation et recherche actions de Natixis en France. Acquisition d'ACG Capital (private equity)

— 2017 Le Groupe devient ODDO BHF

— 2016 Acquisition de BHF-Bank

— 2015 Acquisition de Meriten Investment Management

— 2014 Acquisition de Close Brother Seydler

— 2012 Ouverture de ODDO Services Suisse

— 2011 Ouverture de ODDO Options Hong Kong et ODDO Services Luxembourg

— 2010 Acquisitions de la Banque d'Orsay (gestion d'actifs et banque privée) et de la Banque Robeco (banque privée)

— 2009 Lancement de l'Institut de Recherche ODDO à Tunis. Réconciliation avec Partanéa

— 2008 Création de la joint-venture La Banque Postale Banque Privée

— 2005 Acquisition de Cyril Finance (gestion d'actifs)

— 2004 Acquisitions des activités européennes d'intermédiation actions du Crédit Lyonnais.

— 2003 Acquisition de NFMDA (gestion privée). Création de Génération Vie, en joint-venture avec Allianz.

— 2000 Acquisition de Pinatton (intermédiation, corporate finance et gestion privée)

— 1997 Acquisition de Delahaye Finance (gestion privée)

— 1987 Philippe ODDO, Gérant.
— 1846 Camille Gautier, agent de change [2]

II.4 ODDO BHF Tunis

ODDO BHF Tunis a été lancé à Tunis début 2009 pour accompagner le développement du département de recherche ODDO Securities dans le domaine de la recherche actions. ODDO Tunis contribue à la couverture de plus de 310 sociétés européennes cotées et au succès de ODDO Securities, cabinet à forte notoriété internationale.
Innovant sur le marché tunisien, ODDO Tunis est en pleine croissance et compte aujourd'hui plus de 100 collaborateurs dont plus de 60 informaticiens. La stratégie d'intégration vise à assurer une croissance rapide des collaborateurs et à les former aux métiers de l'analyse financière et à la méthodologie ODDO. Avec un salon international, des formations exigeantes, une culture d'excellence et une réelle dynamique de croissance, ODDO Tunis représente aujourd'hui une opportunité unique à Tunis, ainsi qu'un véritable tremplin de carrière dans les métiers de la finance.

Figure 1.2 - ODDO BHF

III. Présentation générale du département ISM

III.1 Présentation générale

Le Département Information Security Management (ISM) chez Oddo BHF est chargé de la protection des informations sensibles de l'entreprise contre les menaces internes et externes. Ce département joue un rôle crucial dans la mise en place de stratégies de sécurité, la gestion des risques, et la conformité aux normes de sécurité internationales. Il assure également la supervision continue des systèmes d'information pour détecter et répondre aux incidents de sécurité.

III.2 Le Security Operations Center (SOC)

Le Security Operations Center (SOC) constitue une composante clé du département ISM. Il est responsable de la surveillance en temps réel des réseaux et des systèmes d'information pour identifier, analyser, et répondre rapidement aux incidents de sécurité. Le SOC utilise des technologies avancées et des processus rigoureux pour protéger les actifs numériques de l'entreprise, assurer la continuité des opérations, et minimiser les impacts des cyber attaques.

III.3 Les équipes de SOC

III.3.1 SOC Engineer

Les SOC Engineers sont responsables de la création des règles de sécurité. Ils conçoivent des politiques de détection et de réponse aux incidents en utilisant des technologies telles que les SIEM.

III.3.2 Control Team

L'équipe de Control se charge de la supervision et du contrôle des systèmes et des processus de sécurité. Leur rôle est de s'assurer que les contrôles de sécurité sont efficaces et respectent les normes établies.

III.3.3 Red Team

L’équipe Red Team réalise des tests de pénétration (pentesting) pour évaluer la sécurité des systèmes et identifier les vulnérabilités. Leur objectif est de simuler des attaques pour tester la résilience des défenses de l'entreprise.

III.3.4 CTI

L’équipe CTI se concentre sur la recherche et l'analyse des menaces informatiques, y compris les malwares. Ils utilisent des cadres tels que MITRE ATT&CK pour comprendre et anticiper les tactiques, techniques et procédures (TTPs) des attaquants.

III.3.5 CSIRT

Le CSIRT est responsable de la détection et de la réponse aux incidents de sécurité, y compris les malwares.

J'ai effectué mon stage au sein de l'équipe CSIRT, où j'ai acquis une expérience précieuse dans la gestion des incidents de sécurité. Je vais détailler les responsabilités spécifiques de cette équipe et comment elle contribue à la sécurité globale de l'entreprise.

IV. Conclusion

En conclusion, ce chapitre a présenté l'organisation de l'entreprise, le département ISM, et les différentes équipes du SOC, en mettant en lumière leurs rôles complémentaires dans la gestion de la sécurité. Le chapitre suivant se concentrera en détail sur le CSIRT

Chapitre 2
L'Équipe CSIRT et analyses des emails

I. Introduction

Ce chapitre explore les différents membres de l'équipe CSIRT et leurs responsabilités respectives, ainsi que la gestion des incidents de phishing. Nous commencerons par une vue d'ensemble des différents membres de l'équipe CSIRT, puis nous plongerons dans l'analyse des emails.

II. L'Équipe CSIRT

Cette section explore les différents membres au sein de l'équipe CSIRT, chacun ayant des responsabilités distinctes pour assurer une réponse efficace aux incidents de sécurité.

II.1 Analystes junior

Les analystes de niveau 1 sont responsables de l'analyse des alertes détectées par la solution SIEM (Security Information and Event Management) QRadar, en utilisant divers outils d'analyse spécifiques à l'entreprise ainsi que des outils open source tels qu'Abuse, WhereGoes, VirusTotal, URLScam, Mxtoolbox. Leur rôle principal consiste à examiner les emails signalés par les clients ou ceux stockés dans l'ECP en raison de la présence de certains mots-clés suspects.

À travers leur analyse, ils déterminent si les emails sont du spam, des tentatives de scam, de la fraude ou des attaques de phishing. Ils évaluent également si les URL, les adresses IP, ou d'autres éléments associés sont malveillants ou non. Toutefois, il est important de noter que bien qu'ils puissent identifier ces menaces, ils ne prennent pas la décision de bloquer ces éléments ; cette action relève des niveaux supérieurs ou des équipes spécialisées.

II.2 Analystes

Les analystes de niveau 2 partagent certaines responsabilités avec ceux du niveau 1, notamment l'analyse des alertes de sécurité. Cependant, ils vont au-delà en prenant des mesures concrètes, telles que le blocage des emails, des URL, des adresses IP, et des fichiers malveillants identifiés**.**

De plus, ils jouent un rôle clé en fournissant des solutions aux problèmes rencontrés par les analystes de niveau 1. Leur expertise leur permet d'intervenir sur des incidents plus complexes et d'assurer une réponse rapide et efficace aux menaces détectées.

II.3 Analyste senior

L'analyste senior joue un rôle crucial dans la gestion de l'équipe d'analystes. Il est responsable de superviser les opérations quotidiennes, d'assurer la coordination entre les différents niveaux, et de garantir que les procédures sont suivies efficacement.

En plus de ses responsabilités de gestion, le team leader intervient directement dans la résolution des problèmes critiques et complexes qui dépassent les capacités des analystes des niveaux inférieurs. Il développe et met en place des stratégies de défense avancées, propose des améliorations aux processus existants, et veille à ce que l'équipe soit bien équipée pour faire face aux nouvelles menaces.

III. L'analyse des Emails

III.1 Les outils d'analyse

Pour détecter et analyser les emails malveillants, plusieurs outils sont utilisés, chacun offrant des fonctionnalités spécifiques :

- **SIEM :** Outils comme QRadar permettent de centraliser les logs et les alertes, facilitant ainsi la détection d'activités suspectes.
- **VirusTotal :** Permet de vérifier les fichiers, les URLs, Les adresses IP et Les hashs sont malveillantes ou non .
- **AbuseIPDB :** Utilisé pour vérifier si une adresse IP est signalée pour des activités malveillantes.
- **URLScan :** Analyse les liens URL dans les emails pour vérifier leur destination et détecter si les liens mènent à des sites potentiellement dangereux.
- **WhereGoes :** est un outil utilisé pour tracer le chemin complet des redirections d'une URL.
- **Mxtoolbox :** est un ensemble d'outils en ligne utilisé principalement pour la gestion et le diagnostic des systèmes de messagerie.

III.2 Analyse des Emails : Processus et Méthodologie

III.2.1 Analyse des En-têtes d'Email

L'analyse des en-têtes d'email est cruciale pour vérifier l'authenticité de l'expéditeur et identifier les signes de falsification. Voici les principaux éléments à examiner grâce à Mxtoolbox :

- **SPF :** Vérifie si l'IP de l'expéditeur est autorisée à envoyer des emails au nom du domaine. Cela aide à détecter les falsifications de l'adresse d'expédition.
- **DKIM :** Utilise une signature numérique pour confirmer que le contenu de l'email n'a pas été modifié depuis son envoi et que le domaine d'expédition est authentique.
- **DMARC :** Fournit des politiques de validation SPF et DKIM et permet aux propriétaires de domaines de recevoir des rapports sur les tentatives de spoofing.
- **Identification de l'Expéditeur :** Analyse les en-têtes pour vérifier l'identité de l'expéditeur et la cohérence avec les informations fournies par le domaine.

III.2.2 Analyse du Corps de l'Email

L'analyse du contenu de l'email permet d'identifier des éléments suspects et de déterminer la nature de l'email :

- **Contenu du Message** : Examine le texte de l'email pour détecter des indices de phishing, comme des demandes de renseignements personnels ou des incitations à cliquer sur des liens douteux.
- **Analyse des URLs** : Vérifie les liens présents dans l'email pour détecter des redirections vers des sites suspects ou malveillants. Cela inclut l'analyse des URL affichées et des liens cachés.

III.2.3 Conclusion et Classification de l'Email

Après avoir analysé les en-têtes et le corps de l'email, il est important de conclure sur la nature de l'email. Si l'email est identifié comme True positif (c'est-à-dire malicieux), il est nécessaire de préciser son type. En revanche, si l'email est un False positif, il convient de le noter en conséquence.

III.3 Types de Emails Malicieux et exemples d'Analyse d'Email

Les emails malveillants se présentent sous diverses formes, chacune ayant des objectifs spécifiques.

III.2.1 Spam

Emails non sollicités envoyés en masse, souvent pour des campagnes publicitaires ou pour saturer les boîtes de réception .

Exemple de spam : publicité non sollicitée pour des produits pharmaceutiques.

Figure 2.1 - Email de spam

III.2.2 Scam

Les emails de type 'scam' sont des messages envoyés dans le but d'explorer les systèmes et d'identifier d'éventuelles vulnérabilités. Ces emails sont souvent conçus pour tromper les destinataires et les inciter à divulguer des informations sensibles.

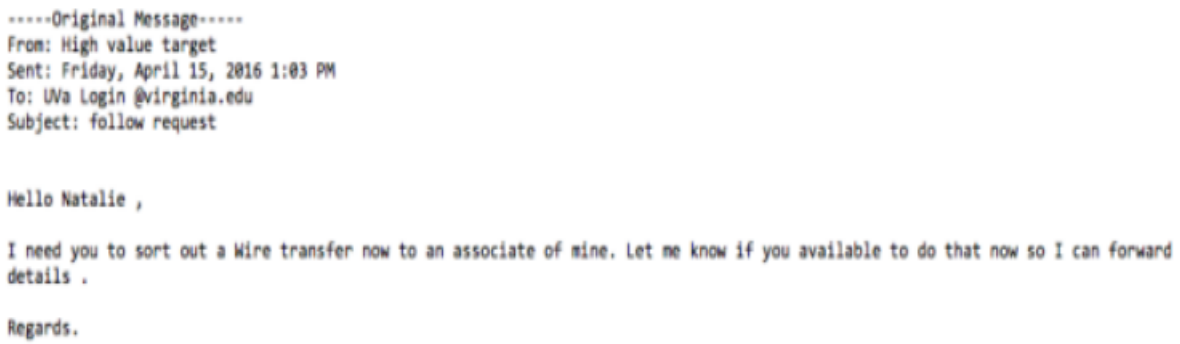


Figure 2.2 - Email de scam

III.2.3 Fraude

Tentatives de tromperie où l'attaquant se fait passer pour une entité légitime afin de recueillir des informations financières ou personnelles.

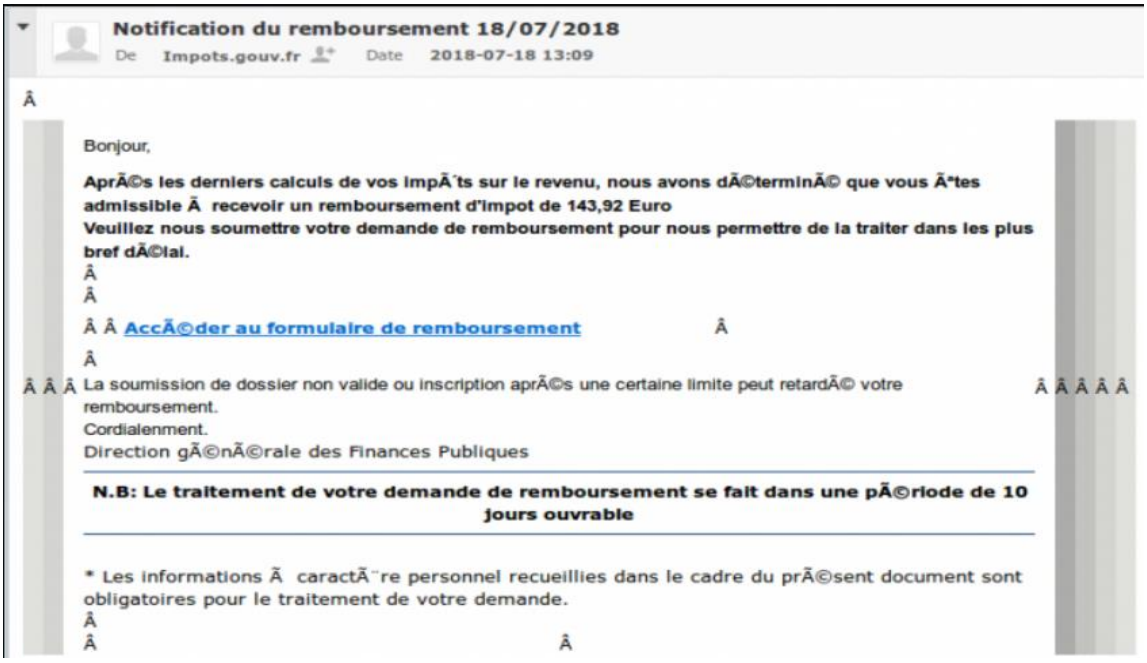


Figure 2.3 - Email de Fraude

III.2.4 phishing

Le « phishing » fait référence à une tentative de vol d'informations sensibles, généralement sous la forme de noms d'utilisateur, de mots de passe, de numéros de carte de crédit, d'informations sur les comptes bancaires ou d'autres données importantes. Le but est de pouvoir utiliser ou vendre ces informations volées. En outre, le phishing est souvent utilisé pour identifier les coordonnées personnelles des employés dans le but de réaliser des attaques ciblées contre leur entreprise. [2]

Les attaques de phishing utilisent généralement des URLs trompeuses et des fichiers malicieux pour tromper les victimes. Ces emails peuvent contenir des liens vers des sites web frauduleux ou des pièces jointes infectées, incitant ainsi les destinataires à fournir des informations sensibles ou à compromettre la sécurité de leurs systèmes.

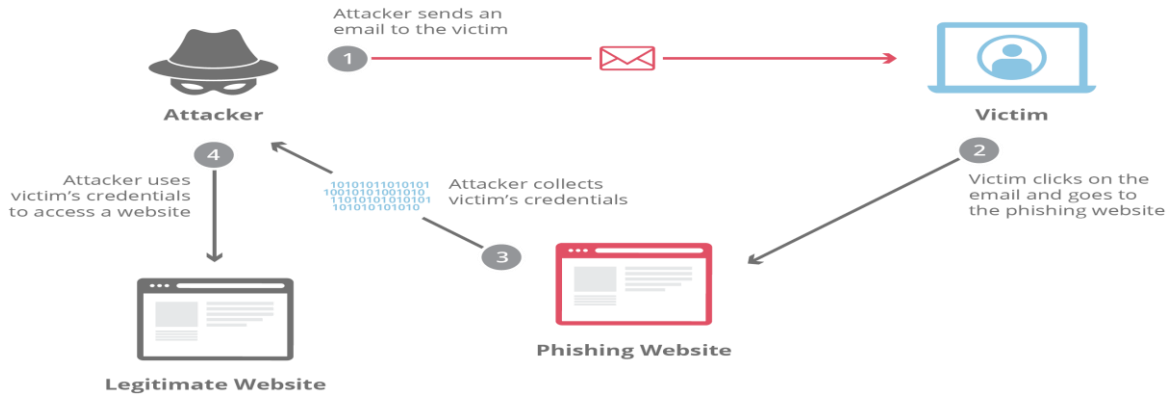


Figure 2.4 - Schéma d'une attaque de phishing

- **Example d'email de phishing :**

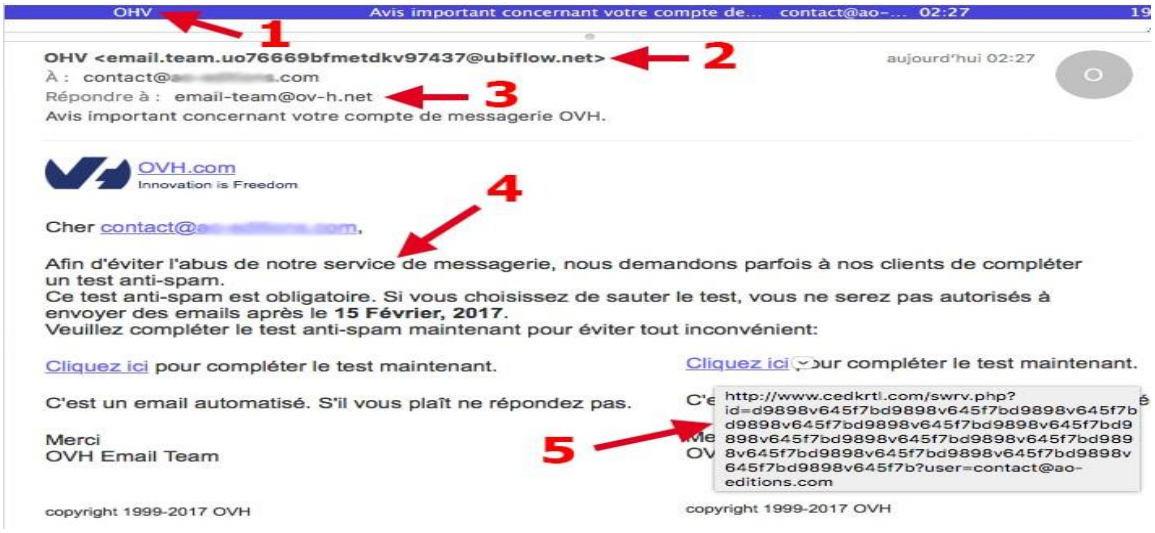


Figure 2.5 - Email de phishing

Cette figure montre que l'absence d'éléments visuels spécifiques et la formulation générique du message peuvent indiquer une tentative de phishing, malgré l'apparence authentique du logo OVH. Pour confirmer si cet email est un phishing, il est essentiel d'examiner l'URL et de vérifier l'adresse email de l'expéditeur.

IV. Conclusion

Dans ce chapitre, j'ai exploré le fonctionnement de l'équipe CSIRT et les méthodes d'analyse des emails, en mettant l'accent sur le phishing, qui repose sur l'utilisation d'URLs et de fichiers malicieux. Cette analyse m'a conduit à développer un script pour analyser les URLs. Le chapitre suivant détaillera ce script et son fonctionnement.

Chapitre 3

Présentation du Script d'Analyse

I. Introduction

Au cours de ce stage, j'ai observé le grand nombre d'emails de phishing contenant des URLs et des pièces jointes, ce qui nécessite une analyse approfondie de la part des analystes. De plus, de nombreux emails présentent des similarités répétitives. Face à cette problématique, j'ai développé un script capable d'analyser non seulement les URLs et les fichiers, mais aussi les hashs et les adresses IP. Dans ce chapitre, je présenterai ce script ainsi que ses fonctionnalités.

II. Outils et Technologies Utilisés

II.1 Langage de Programmation

Python : Python a été choisi comme langage principal pour le développement du script en raison de sa richesse en bibliothèques et de sa flexibilité. Il est particulièrement adapté pour les tâches de traitement de données et d'intégration avec des bases de données.

II.2 Environnements de Développement

VMware : VMware a été utilisé pour créer des environnements virtuels isolés afin de tester et développer le script dans un cadre contrôlé, garantissant ainsi la sécurité et l'intégrité des systèmes en cours d'analyse.

Kali Linux : Kali Linux a servi comme système d'exploitation pour le développement et le test du script. Il fournit une large gamme d'outils de cybersécurité et est particulièrement adapté aux environnements d'analyse de sécurité.

II.3 Bibliothèques et Modules Python

- **requests** : Permet de faire des requêtes HTTP pour interagir avec des services web, comme les API de VirusTotal pour la vérification des URLs et des adresses IP.

- **base64** : Utilisé pour l'encodage et le décodage des données en base64, souvent nécessaire pour le traitement des fichiers et des données.

- **json** : Pour la manipulation des données au format JSON, couramment utilisé pour interagir avec les API et stocker les résultats d'analyse.

- **hashlib** : Fournit des fonctions pour créer des hash (MD5, SHA-256, etc.), utile pour la vérification de l'intégrité des fichiers et des données.

- **argparse** : Gère les arguments en ligne de commande, permettant de rendre le script plus flexible et configurable.

- **sqlalchemy** : Utilisé pour la gestion des bases de données relationnelles. Inclut :

-create_engine : Pour créer la connexion à la base de données.

-Column, Integer, String : Définition des colonnes dans les tables de la base de donnés

-declarative_base : Base pour la définition des modèles de données.

-sessionmaker : Pour créer des sessions de base de données.

- **datetime** : Pour la gestion et le formatage des dates et heures dans le script.

- **prettytable** : Pour afficher les résultats de manière tabulaire et lisible.

- **collections.Counter** : Pour compter et analyser les fréquences des éléments dans les données.

- **plotly.graph_objects** : Pour la création de visualisations graphiques, telles que les graphiques en secteurs (pie charts).

- **Flask** : Utilisé pour créer une interface web permettant aux utilisateurs de consulter les résultats des analyses via une application web. Les modules associés incluent :

  -Flask : Le framework web pour la création de l'application.

  -render_template : Pour rendre les templates HTML.

  -request : Pour traiter les requêtes HTTP dans l'application web.

II.3 Présentation des Fonctions du Script

II.3.1 Fonction pour tester l'URL

```
def url_test(url):
    """
    Analyse une URL en utilisant l'API de VirusTotal et stocke les résultats.
    """
    # Encode l'URL pour l'utiliser dans l'API de VirusTotal
    url_id = base64.urlsafe_b64encode(url.encode()).decode().rstrip("=")

    # Envoie une requête POST à l'API de VirusTotal pour soumettre l'URL
    response = requests.post(
        "https://www.virustotal.com/api/v3/urls",
        headers=headers,
        data=json.dumps({"url": url})
    )

    # Récupère les résultats de l'analyse de l'URL
    result = requests.get(f"https://www.virustotal.com/api/v3/urls/{url_id}",
headers=headers).json()

    # Affiche les résultats de l'analyse
    display_data(result)

    # Extrait la valeur de malveillance de l'analyse
    malicious = result['data']['attributes']['last_analysis_stats']['malicious']

    # Insère les résultats dans la base de données
    insert_analysis(url, "URL", url_id, malicious)

'''
```

II.3.2 Fonction pour tester l'adresse IP

```
def ip_test(ip):
    """
    Analyse une adresse IP en utilisant l'API de VirusTotal et stocke les résultats
    """
    # Récupère les résultats de l'analyse de l'adresse IP
    result = requests.get(f"https://www.virustotal.com/api/v3/ip_addresses/{ip}",
headers=headers).json()

    # Affiche les résultats de l'analyse
    display_data(result)

    # Extrait la valeur de malveillance de l'analyse
    malicious = result['data']['attributes']['last_analysis_stats']['malicious']

    # Crée un hash SHA-256 de l'adresse IP pour le stockage
    ip_bytes = ip.encode('utf-8')
    ip_hash = hashlib.sha256(ip_bytes).hexdigest()

    # Insère les résultats dans la base de données
    insert_analysis(ip, "IP", ip_hash, malicious)
```

II.3.3 Fonction pour tester le fichier

```
def file_test(file_path):
    """
    Analyse un fichier en utilisant l'API de VirusTotal et stocke les résultats.
    """
    # Télécharge le fichier et obtient son identifiant
    file_id = upload_file(file_path)

    # Récupère les résultats de l'analyse du fichier
    result = requests.get(f"https://www.virustotal.com/api/v3/files/{file_id}",
headers=headers).json()

    # Affiche les résultats de l'analyse
    display_data(result)

    # Extrait la valeur de malveillance de l'analyse
    malicious = result['data']['attributes']['last_analysis_stats']['malicious']

    # Insère les résultats dans la base de données
    insert_analysis(file_path, "File", file_id, malicious)
```

II.3.4 Fonction pour tester le hash

```
def hash_test(hash_value):
    """
    Analyse un hash en utilisant l'API de VirusTotal et stocke les résultats.
    """
    # Récupère les résultats de l'analyse du hash
    result = requests.get(f"https://www.virustotal.com/api/v3/files/{hash_value}",
headers=headers).json()

    # Extrait la valeur de malveillance de l'analyse
    malicious = result['data']['attributes']['last_analysis_stats']['malicious']

    # Insère les résultats dans la base de données
    insert_analysis(hash_value, "Hash", hash_value, malicious)

    # Affiche les résultats de l'analyse
    display_data(result)
```

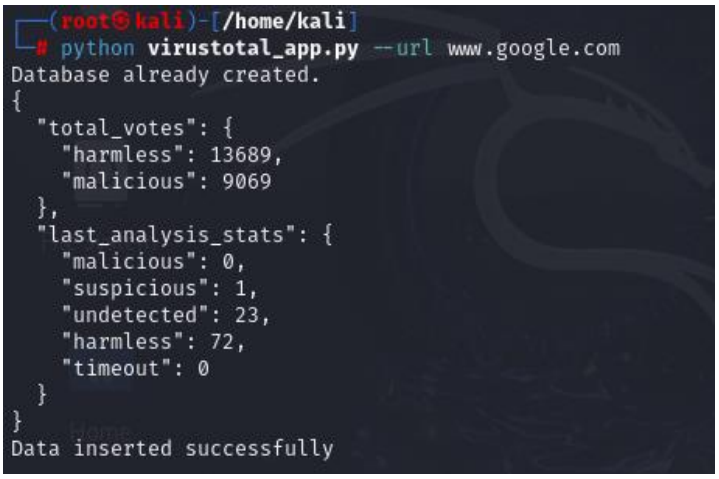
II.4 Stockage des Données

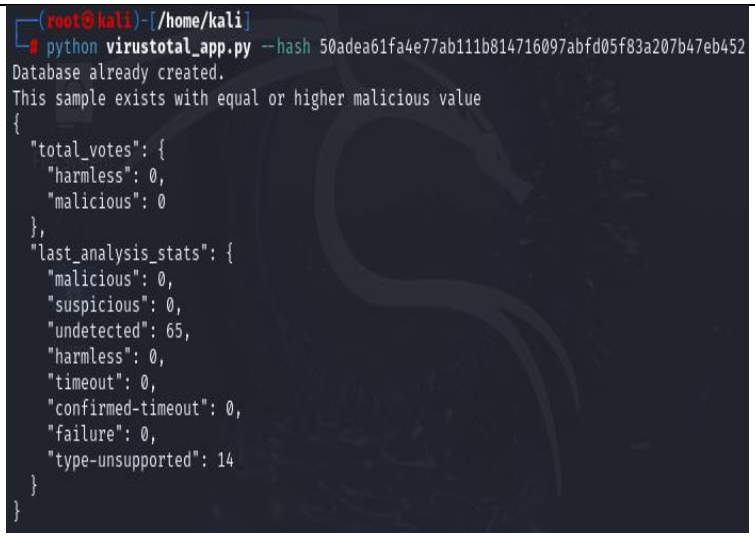
```
app = Flask(__name__)

@app.route('/', methods=['GET', 'POST'])
def index():
    if request.method == 'POST':
        # Vous pouvez ajouter ici du code pour traiter les données envoyées par le
formulaire
        pass

    # Récupérer les analyses depuis la base de données
    analyses = session.query(Analysis).all()
    table_data = [
        {
            'id': analysis.id,
            'sample': analysis.sample,
            'type': analysis.type,
            'hash': analysis.hash,
            'malicious': analysis.malicious,
            'created_time': analysis.created_time.strftime("%d/%m/%Y")
        }
        for analysis in analyses
    ]

    # Créer le diagramme en secteurs
    pie_chart = create_pie_chart()

    # Rendre le template avec les données de la table et le diagramme
    return render_template('index.html', table_data=table_data, pie_chart=pie_chart)
```

Ce code configure une route Flask pour afficher une page web qui récupère les analyses depuis une base de données, les présente sous forme de tableau, génère un diagramme en secteurs, et rend le tout dans un template HTML nommé **index.html**.

III. Fonctionnalité de Script

Le script développé propose plusieurs options permettant d'effectuer des analyses spécifiques et de visualiser les résultats. Voici un aperçu des principales options disponibles :

Option	**Description**	**Capture de Résultats**
--url	Permet de tester une URL en la soumettant à l'API de VirusTotal pour obtenir un rapport détaillé de son analyse	
--ip	Permet de tester une adresse IP en vérifiant sa réputation et ses caractéristiques via l'API de VirusTotal.	

--hash	Permet de tester un hash (par exemple, SHA-256) pour vérifier s'il correspond à un fichier connu et analyser sa sécurité.	
--file	Permet de tester un fichier en l'envoyant à VirusTotal pour une analyse approfondie.	
--history	Affiche l'historique complet des analyses précédemment effectuées, en les récupérant depuis la base de données.	

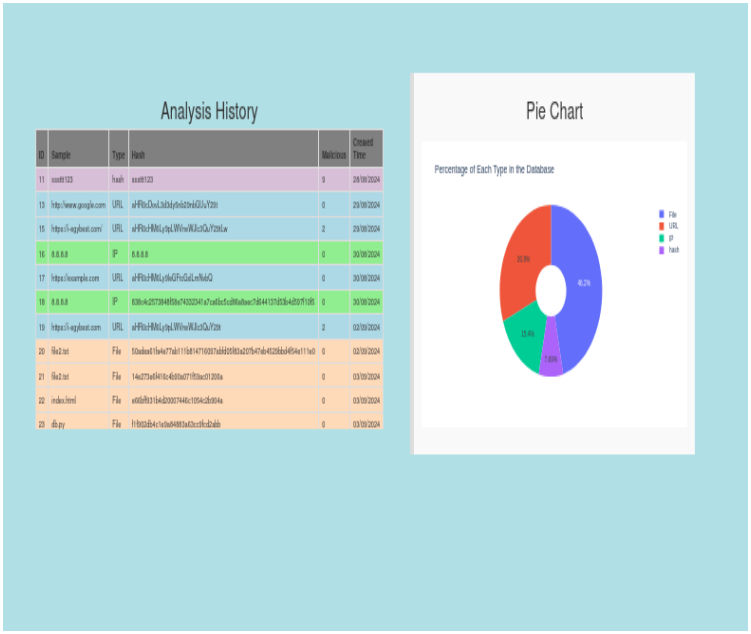
--web	Affiche la table des analyses et le diagramme en secteurs dans une page web, offrant une interface visuelle pour les données.	

Tableau 1- Tableau des options du script et captures de résultats

Ces options permettent aux utilisateurs d'adapter l'utilisation du script en fonction de leurs besoins, offrant à la fois des fonctionnalités d'analyse et des outils de visualisation pour faciliter la gestion des données de cybersécurité.

IV .Conclusion

Ce script simplifie l'analyse des menaces en automatisant la gestion des URLs, fichiers, IPs et hash, tout en centralisant les résultats dans une base de données. Il améliore ainsi l'efficacité des analystes en leur offrant un accès rapide et visuel aux données critiques.

Conclusion générale

Ce rapport a mis en lumière l'importance de l'analyse des menaces dans le contexte de la cybersécurité, en particulier face aux attaques de phishing. Grâce à l'observation des processus au sein du département ISM d'ODDO BHF, j'ai pu développer un script qui automatise l'analyse des URLs, fichiers, adresses IP et hash, tout en centralisant les résultats dans une base de données. Ce script contribue à une gestion plus efficace des menaces, en offrant aux analystes un outil pratique pour consulter l'historique des analyses et visualiser les données.

Pour améliorer davantage ce script, l'objectif futur est de le rendre capable d'analyser les emails dans leur intégralité, y compris les en-têtes, afin de déterminer automatiquement si un email est malicieux ou non. Cette fonctionnalité permettrait d'identifier rapidement les tentatives de phishing en examinant les éléments clés tels que les adresses d'expéditeur, les signatures SPF et DKIM, ainsi que les liens contenus dans les emails. Cette amélioration renforcerait l'efficacité des analystes en automatisant une partie encore plus large de leur travail d'investigation.

Bibliographie

[1] [https://www.oddo-bhf.com/fr/pd/1350/quisommesnous/1378/identite]

[2] [https://www.oddo-bhf.com/fr/pd/1350/quisommesnous/1139/histoire]

[3] [https://www.cloudflare.com/fr-fr/learning/access-management/phishing-attack/]