

**Contournement des systèmes de prévention de la perte de données (DLP) par exfiltration de données en mode air-gap via la technologie Qrcode.**

|  |
| --- |
| Par Alain NICOLAS  2022/2023  Université de Technologie TROYES  Thèse professionnelle de Mastère Spécialisé® Expert en Cybersécurité    Tuteur : Alain CORPEL |

Résumé exécutif

Un executive summary, également appelé résumé exécutif, est un résumé succinct et condensé d'un document ou d'un rapport qui vise à fournir aux décideurs et aux dirigeants une vue d'ensemble rapide des informations clés, des principales conclusions et des recommandations essentielles. Il est généralement utilisé dans un contexte professionnel ou organisationnel pour permettre aux destinataires occupés de comprendre rapidement les aspects les plus importants d'un document sans avoir à lire l'intégralité du contenu.

L'executive summary se trouve généralement au début du document, après la page de titre, mais avant le contenu détaillé. Il est rédigé de manière concise et précise, et il est souvent limité à une ou deux pages, selon les exigences spécifiques.

Dans un executive summary, vous devez inclure les éléments suivants :

1. Contexte et objectifs : Présentez le contexte de la problématique abordée dans le document et expliquez les objectifs principaux de l'étude ou du rapport.

2. Méthodologie : Résumez brièvement les méthodes de recherche ou les approches utilisées pour collecter les données et analyser les informations.

3. Principales conclusions : Résumez les résultats et les principales conclusions de l'étude ou du rapport. Mettez en évidence les découvertes les plus importantes, les tendances clés ou les faits saillants.

4. Recommandations : Présentez de manière concise les principales recommandations ou actions proposées à la suite des conclusions. Indiquez les mesures spécifiques à prendre ou les décisions à prendre pour résoudre la problématique ou pour mettre en œuvre les améliorations suggérées.

5. Implications et impacts : Discutez brièvement des implications stratégiques, des avantages potentiels ou des impacts attendus des recommandations. Mettez en évidence les bénéfices attendus et les résultats escomptés.

L'executive summary doit être rédigé de manière claire, concise et persuasif, en utilisant un langage simple et accessible. Il doit capter l'attention des lecteurs et leur donner une compréhension rapide des points clés du document, afin qu'ils puissent prendre des décisions éclairées en fonction des informations présentées.

Il est important de noter que l'executive summary est généralement destiné à un public spécifique, souvent des décideurs ou des hauts responsables, et il doit donc être adapté à leurs besoins et à leurs préoccupations spécifiques.

**Table des matières**

[Résumé exécutif 2](#__RefHeading___Toc529_829255459)

[1. Introduction 5](#__RefHeading___Toc306_829255459)

[1.1. Contexte et importance de la protection des données d'entreprise 5](#__RefHeading___Toc313_829255459)

[1.2. Risques potentiels liés à l'utilisation malveillante des QR codes et des webcams intégrées 5](#__RefHeading___Toc315_829255459)

[1.3. Objectif de la thèse : démontrer la faisabilité de l'exfiltration de données via les QR codes et les webcams intégrées, contournant les systèmes DLP 5](#__RefHeading___Toc317_829255459)

[2. État de l'art et revue de littérature 5](#__RefHeading___Toc308_829255459)

[2.1. Méthodes d'exfiltration de données existantes 5](#__RefHeading___Toc313_829255459_Copie_1)

[2.2. Technologies des QR codes et reconnaissance d'image 5](#__RefHeading___Toc313_829255459_Copie_1_Copie_1)

[2.3. Systèmes DLP et leur efficacité dans la détection de l'exfiltration de données 5](#__RefHeading___Toc313_829255459_Copie_1_Copie_2)

[2.4. Travaux de recherche connexes dans la cybersécurité et l'exfiltration de données 5](#__RefHeading___Toc313_829255459_Copie_1_Copie_2_Copie_2)

[3. Méthodologie 5](#__RefHeading___Toc308_829255459_Copie_1)

[3.1. Description détaillée des deux modèles proposés pour l'exfiltration de données via QR codes et webcams intégrées 5](#__RefHeading___Toc313_829255459_Copie_1_Copie_3)

[3.2. Évaluation et mesure des débits attendus pour chaque modèle, en prenant en compte différents formats de données et contraintes techniques 5](#__RefHeading___Toc313_829255459_Copie_1_Copie_1_Copie_1)

[3.3. Scénarios d'expérimentation et paramètres pris en considération 5](#__RefHeading___Toc313_829255459_Copie_1_Copie_2_Copie_1)

[4. Résultats 6](#__RefHeading___Toc308_829255459_Copie_1_Copie_1)

[4.1. Présentation des résultats des expérimentations, détaillant les débits obtenus pour chaque modèle et format de données 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_3_Copie_1)

[4.2. Analyse des résultats et discussion de leur signification, mise en évidence des vulnérabilités et des risques associés à l'exfiltration de données via cette méthode 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_1_Copie_1_Copie_1)

[4.3. Identification des vulnérabilités et des risques potentiels 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_2_Copie_1_Copie_1)

[5. Contre-mesures 6](#__RefHeading___Toc308_829255459_Copie_1_Copie_2)

[5.1. Proposition de contre-mesures efficaces pour prévenir et détecter l'exfiltration de données via les QR codes et les webcams intégrées 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_3_Copie_2)

[5.2. Discussion des stratégies de sécurité, des bonnes pratiques et des technologies complémentaires pour renforcer la protection des données d'entreprise 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_1_Copie_1_Copie_2)

[5.3. Sensibilisation des employés et formation à la sécurité 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_2_Copie_1_Copie_2)

[6. Conclusion 6](#__RefHeading___Toc308_829255459_Copie_1_Copie_3)

[6.1. Résumé des principaux résultats et conclusions de la thèse 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_3_Copie_3)

[6.2. Mise en avant de l'importance de sensibiliser les entreprises à cette vulnérabilité et d'implémenter des mesures de sécurité adéquates 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_1_Copie_1_Copie_3)

[6.3. Mise en avant de l'importance de sensibiliser les entreprises à cette vulnérabilité et d'implémenter des mesures de sécurité adéquates 6](#__RefHeading___Toc313_829255459_Copie_1_Copie_2_Copie_1_Copie_3)

"Étude approfondie de l'exfiltration de données sensibles dans les environnements de télétravail : Analyse des nouveaux vecteurs basés sur QR codes et capteurs de la caméra, et développement d'une approche de détection et de prévention avancée""

Résumé (Executive Summary) : Cette thèse professionnelle vise à examiner les risques liés à l'exfiltration de données sensibles dans les environnements de télétravail en utilisant des vecteurs émergents tels que les QR codes et les capteurs de la caméra. Elle explore les limites des solutions de prévention courantes, telles que le blocage de l'utilisation de clés USB, le filtrage des e-mails et des sorties imprimantes, et propose des mesures de mitigation pour contrer ces nouvelles méthodes d'exfiltration.

La méthodologie adoptée comprend une analyse approfondie de la littérature et de l'état de l'art, suivie d'une évaluation des techniques de communication via les QR codes et les capteurs de la caméra. Une simulation est réalisée pour évaluer l'efficacité de ces méthodes d'exfiltration et pour identifier les vulnérabilités potentielles. Sur la base des résultats obtenus, une approche de solution est proposée, incluant des recommandations pour les politiques et les stratégies de prévention des fuites de données sensibles dans les environnements de télétravail.

La thèse professionnelle met en évidence les défis spécifiques posés par l'utilisation des QR codes et des capteurs de la caméra, en particulier dans le contexte du télétravail. Elle présente également des mesures techniques et organisationnelles pour renforcer la sécurité des données sensibles, notamment la sensibilisation des employés, la surveillance des communications et la mise en place de politiques de sécurité adaptées.

Mots-clés : exfiltration de données, télétravail, QR codes, capteurs de la caméra, prévention des fuites de données, sécurité des données sensibles.

Références

La thèse professionnelle sera rédigée dans un style académique universitaire, en respectant les normes de rédaction scientifique. Les illustrations, graphiques et schémas pertinents seront inclus et correctement référencés. La qualité d'expression écrite sera soignée, avec une formulation claire, persuasive et synthétique. La déontologie des sources sera respectée, en fournissant une bibliographie précise qui reflète l'état de l'art dans le domaine de la prévention des fuites de données et de la cybersécurité.

Glossaire :

# Introduction

## Contexte et importance de la protection des données d'entreprise

## Risques potentiels liés à l'utilisation malveillante des QR codes et des webcams intégrées

## Objectif de la thèse : démontrer la faisabilité de l'exfiltration de données via les QR codes et les webcams intégrées, contournant les systèmes DLP

# État de l'art et revue de littérature

## Méthodes d'exfiltration de données existantes

## Technologies des QR codes et reconnaissance d'image

## Systèmes DLP et leur efficacité dans la détection de l'exfiltration de données

## Travaux de recherche connexes dans la cybersécurité et l'exfiltration de données

# Méthodologie

## Description détaillée des deux modèles proposés pour l'exfiltration de données via QR codes et webcams intégrées

## Évaluation et mesure des débits attendus pour chaque modèle, en prenant en compte différents formats de données et contraintes techniques

## Scénarios d'expérimentation et paramètres pris en considération

# Résultats

## Présentation des résultats des expérimentations, détaillant les débits obtenus pour chaque modèle et format de données

## Analyse des résultats et discussion de leur signification, mise en évidence des vulnérabilités et des risques associés à l'exfiltration de données via cette méthode

## Identification des vulnérabilités et des risques potentiels

# Contre-mesures

## Proposition de contre-mesures efficaces pour prévenir et détecter l'exfiltration de données via les QR codes et les webcams intégrées

## Discussion des stratégies de sécurité, des bonnes pratiques et des technologies complémentaires pour renforcer la protection des données d'entreprise

## Sensibilisation des employés et formation à la sécurité

# Conclusion

## Résumé des principaux résultats et conclusions de la thèse

## Mise en avant de l'importance de sensibiliser les entreprises à cette vulnérabilité et d'implémenter des mesures de sécurité adéquates

## Mise en avant de l'importance de sensibiliser les entreprises à cette vulnérabilité et d'implémenter des mesures de sécurité adéquates

https://www.futura-sciences.com/tech/actualites/securite-pirater-ordinateur-via-led-son-disque-dur-cest-possible-66433/

https://www.scitepress.org/papers/2014/51204/51204.pdf

Glossaire :

Air gap : En [sécurité informatique](https://fr.wikipedia.org/wiki/Sécurité_informatique), un air gap, aussi appelé air wall, est une mesure de sécurité consistant à isoler physiquement un système à sécuriser de tout [réseau informatique](https://fr.wikipedia.org/wiki/Réseau_informatique). Cette mesure, lorsqu'elle est correctement implémentée, rend toute tentative de piratage à distance impossible, quelle que soit sa sophistication.