LOGO ORGANISME ACADEMIQUE

ADISCA N°	
Date du rapport de stage :	**19/03/2025**

MEMOIRE TECHNIQUE ARIANEGROUP

TITRE DU RAPPORT :	Levée de doute sur un produit industriel
APPPRENTI :	Maxime Laville
Date de l'alternance :	Du 04/12/2023 au 31/07/2025
TUTEUR D'ENTREPRISE :	**R.L**
Service :	Systems & Products CyberSecurity Engineer
ORGANISME D'ACCUEIL :	**ARIANEGROUP**
Adresse :	51/61 route de Verneuil BP71040 78131 LES MUREAUX CEDEX
ORGANISME ACADEMIQUE :	Aurlom BTS+
Adresse :	118 Avenue Jean Jaurès 75019, PARIS
TUTEUR PEDAGOGIQUE :	Corentin, DAGUET

Exemplaire Papier n° 1/ Y : Prénom, Nom
Exemplaire Papier n° 2/ Y : Prénom, Nom
Exemplaire Papier n° 3/ Y : Prénom, Nom
Exemplaire Papier n° 4/ Y : Prénom, Nom
Exemplaire Papier n° 5/ Y : Prénom, Nom
Exemplaire Papier n° 6/ Y : Prénom, Nom

MENTION DE PROPRIETE

Ce document et les informations qu'il contient sont propriété d'ArianeGroup. Il ne doit pas être utilisé à d'autres fins que celles pour lesquelles il a été remis. Il ne peut être ni reproduit, ni divulgué à des tiers (en tout ou partie) sans l'accord préalable et écrit d'ArianeGroup. ArianeGroup SAS –Tous droits réservés. // This document and the information it contains are property of ArianeGroup. It shall not be used for any purpose other than those for which it was supplied. It shall not be repro-duced or disclosed (in whole or in part) to any third party without ArianeGroup prior written consent. ArianeGroup SAS – All rights reserved.

CLAUSE DE DEONTOLOGIE

Les activités d'ArianeGroup intéressent la défense et la sécurité nationale et les intérêts fondamentaux de la nation. Ses salariés et sous-traitants sont soumis à un devoir de discrétion professionnelle et ne sont pas autorisés à diffuser ou rendre accessible ces informations à des personnes ou organismes non-autorisés. Les informations auxquelles j'ai eu l'accès pendant mon apprentissage en entreprise sont non-publiques, voire confidentielles.

De fait, ce document à vocation académique ne comporte aucun nom et chiffres réels. Les informations qu'il contient sont propriété d'ArianeGroup. Il ne doit pas être utilisé à d'autres fins que celles pour lesquelles il a été remis. Il ne peut être ni reproduit, ni divulgué à des tiers (en tout ou partie) sans l'accord préalable et écrit d'ArianeGroup SAS.

2025/2025

Mission professionnelle N°1

LAVILLE, Maxime

ArianeGroup

19/03/2025

Levée de doute sur un produit industriel

Description :
Cette mission consiste à définir un processus afin de s'assurer que les alertes remontées par l'analyse antivirale ne représentent pas un risque cybersécurité vraissemblable.

Validation de la mission professionnelle :

Nom	Date	Tampon
Maxime Laville	19/03/2025	

S o m m a i r e

Table des illustrations

1 FORMALISATION DU BESOIN

Il est nécessaire de s'assurer régulièrement que les supports des produits industriels n'aient pas été infectés par des programmes malveillants afin de garantir la disponibilité, l'intégrité et la confidentialité des données de ces produits.

Dans ce but, des analyses anti-virales sont réalisées et peuvent faire remonter des alertes qui doivent être analysées par l'équipe cybersécurité. Une note de levée de doute est ainsi rédigée afin d'expliquer pourquoi les alertes levées par les anti-virus sont considérées comme de faux positifs et garantir une traçabilité de cette démarche.

2 ANALYSE ANTIVIRALE

L’analyse antivirale est un processus essentiel pour identifier et neutraliser les menaces informatiques susceptibles de compromettre la sécurité des systèmes d’information. Elle permet de détecter, analyser et signaler toute activité malveillante qui pourrait affecter l’intégrité, la confidentialité ou la disponibilité des données. Parmi les types de menaces que cette analyse peut détecter, on retrouve notamment :

- **Logiciels malveillants (malwares)** : Ce terme englobe toutes les applications ou programmes conçus pour nuire aux systèmes, voler des informations, ou perturber les activités des utilisateurs.
- **Les virus** : Ce sont des programmes capables de se propager d’un système à un autre en infectant des fichiers légitimes. Une fois actifs, ils peuvent endommager des données, ralentir les systèmes ou entraîner des pertes d'informations.
- **Les ransomwares** : Ces logiciels chiffrent les données d'un utilisateur ou d’une organisation et exigent le paiement d'une rançon pour en restaurer l’accès. Les attaques par ransomware sont de plus en plus courantes et peuvent avoir des conséquences graves sur l’activité des entreprises.
- **Les logiciels espions (spywares)** : Ces programmes collectent secrètement des informations sur les utilisateurs, souvent à des fins de surveillance ou de vol de données sensibles, sans que la victime en ait conscience.

Dans le cadre d'une levée de doute, ces analyses antivirales jouent un rôle crucial. Elles servent de données d’entrées pour réaliser cette analyse et générer le rapport de levée de doute, document permettant de confirmer ou d'infirmer l'existence d'une menace avérée.

2.1 DESCRIPTION DE LA LEVEE DE DOUTE

Le terme de levée de doute est une opération qui consiste à évaluer la vraissemblance des menaces remontées par une analyse antivirus.

La levée de doute est constituée des parties suivantes :

- **L'objet :** présentation de l'objectif du document
- **Produit :** présentation des produits analysés, on y retrouve le nom du produit, son numéro de série et le média.
- **Contexte de l'analyse antivirale :** pour chacun des produits, il y aura la date de l'analyse, son identifiant, le nom de la station utilisée, le logiciel de la station blanche, la version du logiciel et la date de la mise à jour antivirale.
- **Menaces :** les noms des différents fichiers mis en cause sont listés dans cette partie.
- **Analyse des menaces :** analyses des menaces effectuées par différents antivirus avec le nom du fichier et le condensat associé.
- **Non scannées :** liste des différents fichiers n'ayant pas été scannés en expliquant pourquoi cela n'a pas été le cas.
- **Conclusion :** s'assurer que l'ensemble des fichiers ne présentent pas de risque pour le produit par le fait que ce soit des faux positifs.

2.2 PROCESSUS D'ACTIVITE

Le processus ci-dessous présente le déroulement des activités sur l'analyse antivirale ainsi que la levée de doute :

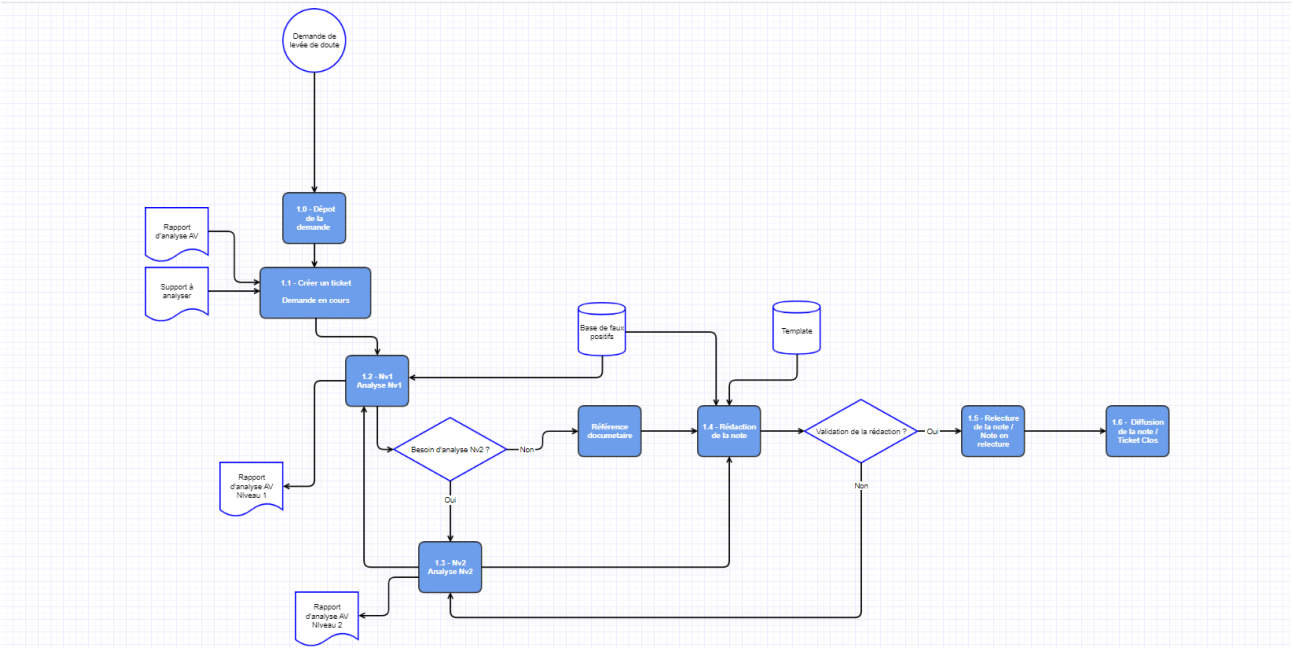


Figure 1 - Processus d'activité de la levée de doute

Activités :

- **Dépôt de la requête sur le réseau**
- **Création d'un ticket**
- **Analyse de niveau 1**
- **Analyse de niveau 2**
- **Rédaction de la note**
- **Relecture de le note**
- **Diffusion de la note**

2.3 DESCRIPTION DES ACTIVITES

Activité 1.0 – Dépôt de la requête sur le réseau : Une demande de levée de doute est initiée et crée sur le réseau.

Activité 1.1 - Création d'un ticket: L'utilisateur remplit le formulaire sur l'espace de gestion des requête « Levée de doute » permettant de génère un ticket. Ce dernier contient les informations suivantes : Nom et prénom, le programme, le projet, etc. La création de ce ticket déclenche l'activité suivante d'analyse de la demande.

Activité 1.2 - Analyse de niveau 1 :

Le 1er niveau de l'analyse antivirale consiste à comparer les condensats, remontés par l'analyse anti-virale, avec la liste des condensats identifiés comme étant de faux positifs, présente dans la base de donnée dédiée. Cette première analyse de niveau 1 permettra de générer un premier rapport d'analyse antivirale.

Activité 1.3 - Analyse de niveau 2 :

Dans le cas où des condensats remontés par l'analyse anti-virale ne sont pas présents dans la base de donnée des faux positifs, une analyse antivirale plus approfondie est réalisée pour identifier la vraissemblance de la menace.

Activité 1.4 - Rédaction de la note.

Une note sera rédigée sur la base du template « note levée de doute » une fois les menaces identifiées et analysées. La note contient les informations suivantes : l'objet de la demande, le produit, l'analyse antivirale, les menaces, l'analyse des menaces, les fichiers non scannés et la conclusion.

La note de levée de doute sera ensuite envoyée en relecture.

Activité 1.5 - Relecture de la note.

La note est relue par le responsable afin de valider la conclusion.

Activité 1.6 – Diffusion de la note.

Diffusion de la note vers le demandeur de la levée de doute.

2.4 NOTE DE LEVEE DE DOUTE

Cette partie présente le template de la levée de doute.

1. **OBJET**

   L'objectif de cette note est d'évaluer la vraissemblance des menaces remontées par l'analyse antivirale du produit **NOM-PRODUIT.**

2. **PRODUIT**

Les produits concernés sont :

Nom du produit	
Numéro de série	
Caractéristique du support	

Tableau 1 – Caractéristique du **Produit 1.**

3. ANALYSE ANTIVIRALE

Les analyses antivirales ont été réalisées avec une station blanche.

Nom de la station	
Logiciel Station	
Version de logiciel	
Date de la dernière mise à jour antivirale de la station	

- Tableau 2 – Caractéristique de la station blanche.

Produit 1 :

Date de l'analyse	
Identifiant de l'analyse	

Tableau 3 – Rapport d'analyse antivirale du **Produit 1**.

Nom	Non scanné (erreur)	Sain	Menace	Mise à jour	Anti-virus	Version logiciel	Etat de l'analyse

1. **Nom :** cette colonne désigne le nom des antivirus utilisés.

2. **Non scanné :** cette colonne désigne le nombre de fichiers non scannés.
3. **Sain :** cette colonne désigne le nombre de fichier sain.
4. **Menace :** cette colonne désigne le nombre de fichiers menaçants détectés.
5. **Mise à jour :** Cette colonne désigne la date à laquelle la mise à jour a été effectuée.
6. **Anti-virus :** Cette colonne désigne le nom du logiciel antivirus.
7. **Version logiciel :** cette colonne désigne la version du logiciel utilisée.
8. **Etat de l'analyse :** Cette colonne désigne l'état de l'analyse par une validation (OK/NOK).

4. MENACES

Les fichiers mis en cause par les différents PV antiviraux et présents sur les supports sont :

Liste des fichiers suspects avec le nom du fichier et le condensat.

5. ANALYSES DES MENACES

Ce chapitre présente l'analyses des menaces identifiées par les différents antivirus.

a. FICHIER 1

A répéter pour chaque fichier.

6. Analyse Cybersecurité

Fichier mis en cause étant un faux positif ou n'est pas un faux positif.

7. NON SCANNES

Liste des différents fichiers n'ayant pas été scannés en expliquant pourquoi cela est considéré comme ne présentant pas de risques.

8. CONCLUSION

S'assurer que l'ensemble des fichiers ne présentent pas de risque pour le produit par le fait que ce soit des faux positifs, soit des fausses menaces.

3 VIRUSTOTAL

VirustTotal est un logiciel disponible sur internet qui permet, sur la base d'un fichier ou de son condensat, de comparer les résultats entre différents antivirus.

Il se présente de la manière suivante :

Figure 2 - Page d'accueil de VirusTotal

Fonctionnalités principales de VirusTotal :

- **Analyse de fichiers**
- **Analyse d'URL**
- **Rapports et Historique**
- **Intégration et API**

3.1 DESCRIPTION DES FONCTIONNALITES

Analyse de fichiers :

Les utilisateurs peuvent envoyer des fichiers (exécutables, documents, scripts, etc.) pour vérifier s'ils contiennent des virus ou d'autres formes de logiciels malveillants. VirusTotal analyse ces fichiers à l'aide de plusieurs moteurs d'antivirus et indique les résultats de chaque moteur.

Analyse d'URL :

VirusTotal permet aussi de vérifier les liens ou les sites web pour détecter des URL suspectes qui pourraient héberger des logiciels malveillants, des arnaques, du phishing, etc.

Rapports et Historique :

Pour chaque fichier ou URL, VirusTotal crée un rapport détaillé qui montre les résultats des différents antivirus, les comportements suspectés, ainsi que l'historique des détections. Les utilisateurs peuvent voir si un fichier ou un lien a déjà été analysé dans le passé.

Intégrations et API :

VirusTotal propose une API (Application Programming Interface) qui permet aux développeurs et aux entreprises d'intégrer ses fonctionnalités dans leurs propres systèmes. Cette API est souvent utilisée pour l'automatisation de la détection de menaces au sein de solutions de sécurité.

3.2 L'ANALYSE DE FICHIERS

Cette partie présente le déroulement d'une analyse de fichiers.

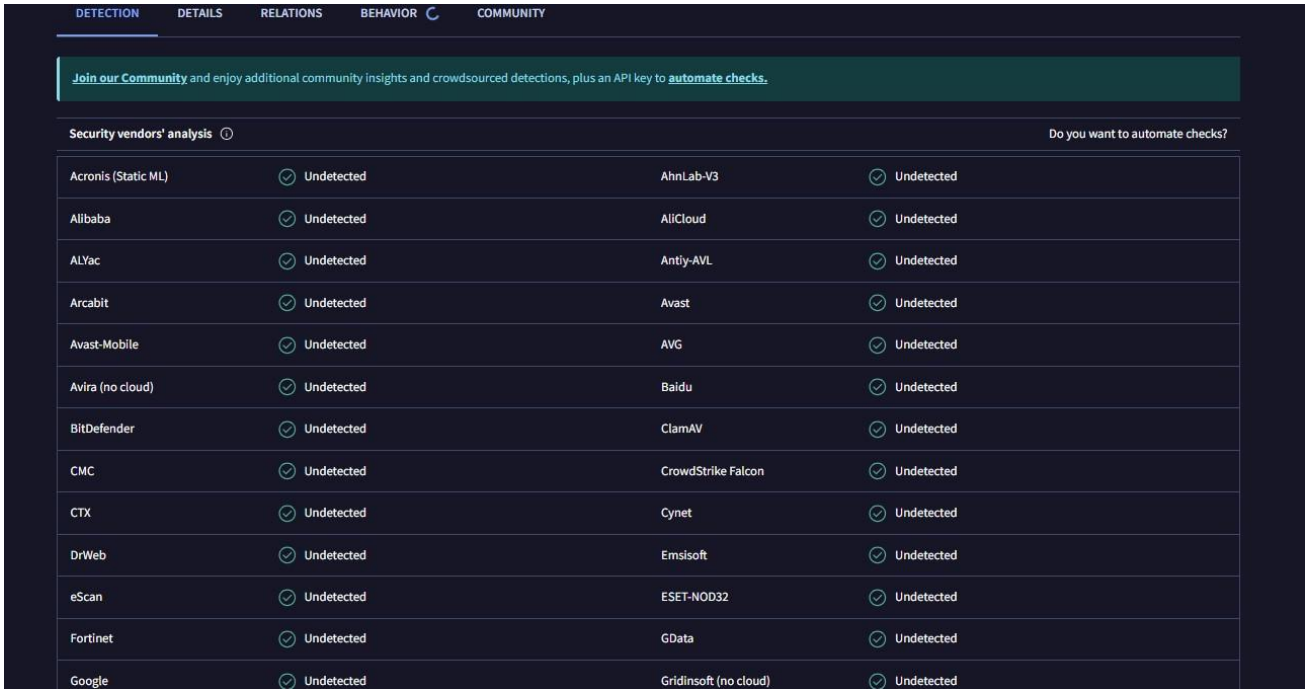


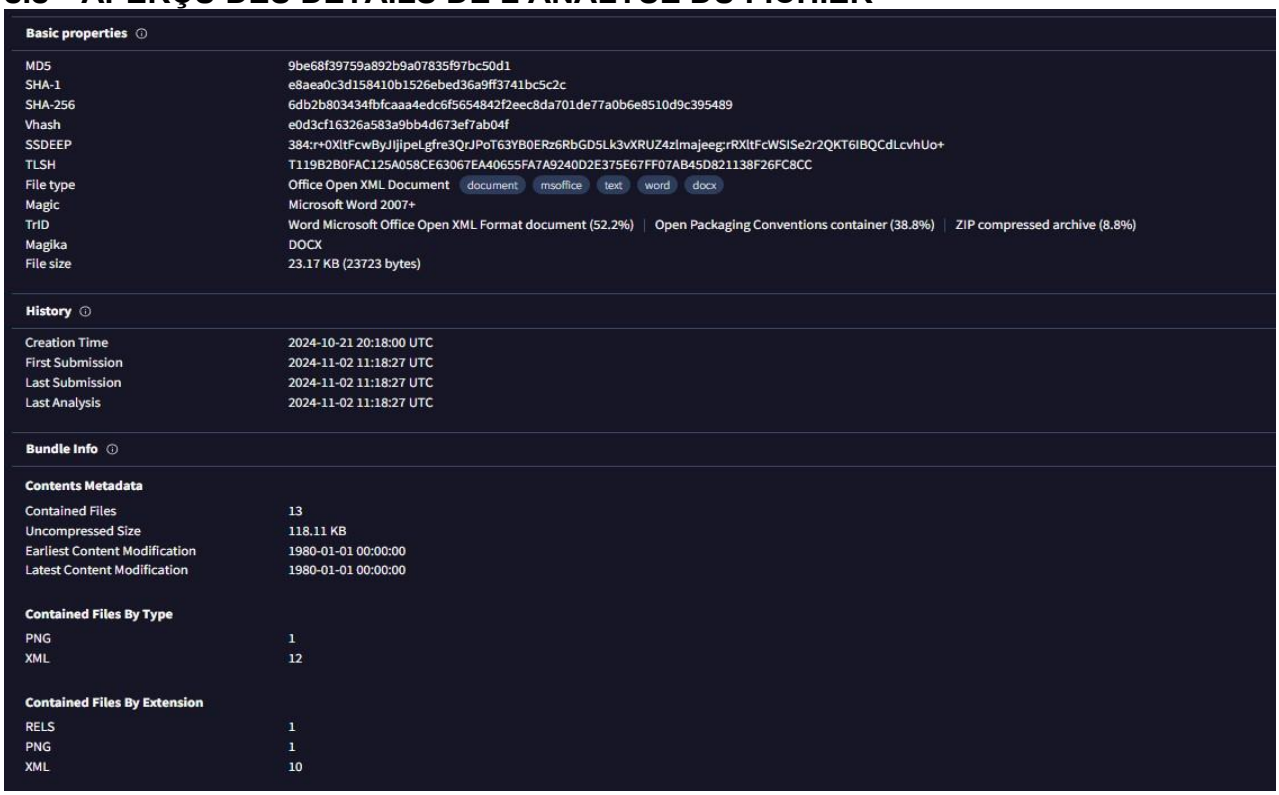
Figure 3 - Liste des fournisseurs de solutions antivirus et de sécurité

Une fois l'analyse du fichier terminée, l'interface présente une liste de divers fournisseurs de solutions antivirales et de sécurité, comme Acronis ou BitDefender, ayant chacun son propre moteur d'analyse.

Pour chaque fournisseur, il est indiqué si une menace a été détectée ou non.

L'ensemble de l'interface nous donne un aperçu des résultats d'analyse de sécurité effectuée par plusieurs logiciel d'antivirus.

3.3 APERÇU DES DETAILS DE L'ANALYSE DU FICHIER



Basic properties

MD5	9be68f39759a892b9a07835f97bc50d1
SHA-1	e8aea0c3d158410b1526ebed36a9ff3741bc5c2c
SHA-256	6db2b803434fbfcaaa4edc6f5654842f2eec8da701de77a0b6e8510d9c395489
Vhash	e0d3cf16326a583a9bb4d673ef7ab04f
SSDEEP	384:r+0XltFcwByJIjipeLgfre3QrJPoT63YB0ERz6RbGD5Lk3vXRUZ4zlmajeeg:rRXltFcWSlSe2r2QKT6IBQCdLcvhUo+
TLSH	T119B2B0FAC125A058CE63067EA40655FA7A9240D2E375E67FF07AB45D821138F26FC8CC
File type	Office Open XML Document document msoffice text word docx
Magic	Microsoft Word 2007+
TrID	Word Microsoft Office Open XML Format document (52.2%) | Open Packaging Conventions container (38.8%) | ZIP compressed archive (8.8%)
Magika	DOCX
File size	23.17 KB (23723 bytes)

History

Creation Time	2024-10-21 20:18:00 UTC
First Submission	2024-11-02 11:18:27 UTC
Last Submission	2024-11-02 11:18:27 UTC
Last Analysis	2024-11-02 11:18:27 UTC

Bundle Info

Contents Metadata

Contained Files	13
Uncompressed Size	118.11 KB
Earliest Content Modification	1980-01-01 00:00:00
Latest Content Modification	1980-01-01 00:00:00

Contained Files By Type

PNG	1
XML	12

Contained Files By Extension

RELS	1
PNG	1
XML	10

Figure 4 - Détails de l'analyse du fichier

Dans la liste des détails, on y retrouve les condensats des différents algorithmes de hachage comme MD5 ou SHA-256, le type du fichier, la taille du fichier, son historique de création et plusieurs autres informations diverses concernant ce fichier.