



Documentation Fonctionnelle

CYBERHAWK

DOCUMENTATION FONCTIONNELLE



SOMMAIRE

1. Introduction	3
1.1 Définitions	3
1.2 Abréviations	4
2. Présentation générale	5
3. Architecture Projet	6
3.1 Architecture globale	6
3.2 Echanges réseaux	7
3.3 Systèmes d'Exploitation	8
3.4 Modules d'analyse	8
4. Fonctionnement général	10
4.1 Envoi de fichiers depuis un media amovible	10
4.2 Récupération de fichiers depuis l'espace personnel	11
5. Mises-à-jour	12
5.1 Préambule	12
5.2 Signatures Antivirales	13
5.3 Antivirus	13
5.4 Code Source CyberHawk	14
5.5 Système d'Exploitations CyberHawk (Offline)	14
6. Gestion des logs	15
6.1 Logs Serveur Principal CyberHawk	15
6.2 Logs serveur de mises-à-jour CyberHawk	15
6.3 Logs miroir	16



1. Introduction

1.1 Définitions

ANTIVIRUS	Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus informatique).
CHIFFREMENT	Le chiffrement (ou cryptage) est un procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement.
CYBERHAWK	Solution NÉOSOFT de SAS de décontamination.
DEBIAN	Debian GNU/Linux est une distribution spécifique du système d'exploitation Linux disposant de nombreux paquets.
FIREWALL	Un pare-feu (de l'anglais Firewall) est un logiciel et / ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets.
LOG	Le terme log désigne un historique d'événements et par extension le fichier contenant cet historique.
SAS	Le SAS est un dispositif qui permet de passer d'un lieu à un autre, d'un environnement à un autre.



1.2 Abréviations

APT	Advanced Package Tool
AV	Antivirus
DMZ	DeMilitarized Zone
FW	Firewall
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
MAJ	Mise-A-Jour
MD5	Message Digest 5
SI	Système d'Information
SHA-1	Secure Hash Algorithm 1
SSH	Secure Shell
TCP	Transmission Control Protocol
USB	Universal Serial Bus



2. Présentation générale

Afin de transférer des fichiers (firmwares, documents, etc.) contenus sur des média amovibles (supports USB) vers des réseaux de confiance (ou à sécurité renforcée), des interventions physiques sur les équipements du réseau sont nécessaires.

La problématique inhérente à cette pratique reste la propagation (automatique ou non) d'éléments potentiellement malveillants à l'intérieur du réseau de confiance. Ces éléments, en fonction de leur niveau de menace, pourraient porter atteinte à la disponibilité, l'intégrité ou encore à la confidentialité de celui-ci.

La solution de SAS NÉOSOFT « CyberHawk » permet de s'affranchir du besoin d'utilisation de médias amovibles à l'intérieur du réseau de confiance, grâce à l'utilisation d'un serveur de décontamination cloisonné, accessible via une interface web d'échange de fichiers.

L'accès à l'interface web de gestion de fichiers peut être mis à disposition sur un système d'information (SI) séparé de moindre importance, ou sur une station dédiée sécurisée (borne libre-service).

Sur CyberHawk, chaque utilisateur est libre de créer son espace personnel et de transférer les fichiers de son choix. Ces fichiers sont ensuite analysés par plusieurs modules (solutions antivirales, routines, Blacklists, etc.) avant d'être stockés (ou supprimés si une menace est détectée par au moins un module).

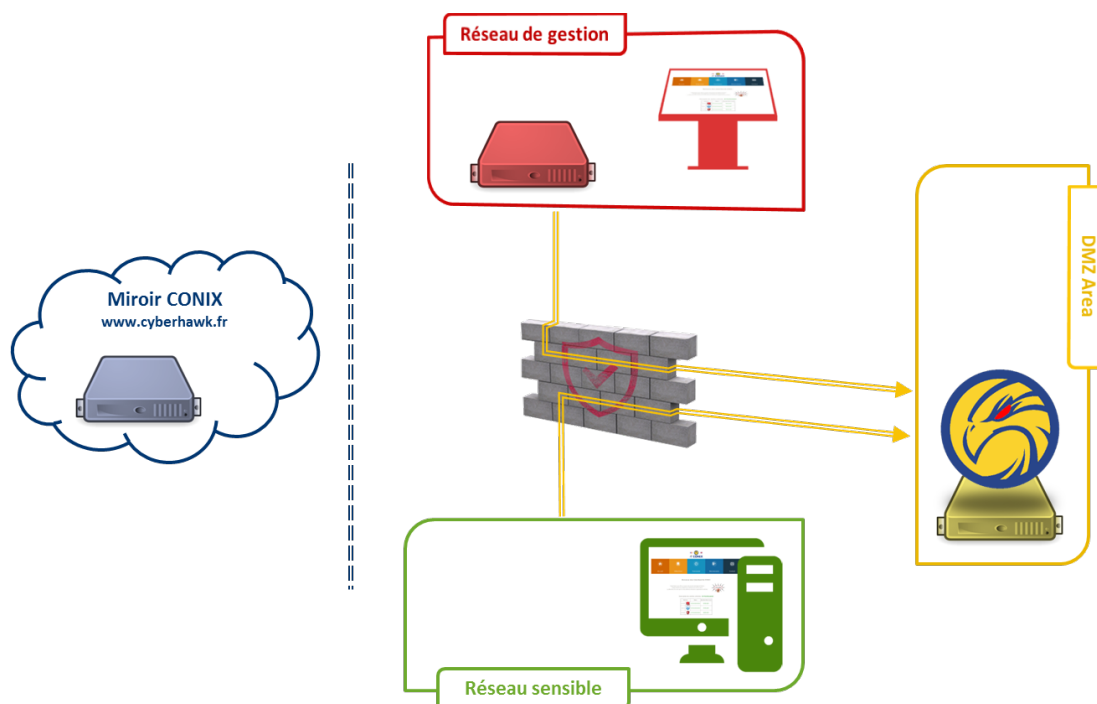
Contrairement aux solutions physiques concurrentes permettant la décontamination de clés USB sur borne, CyberHawk permet une décontamination via le réseau quel que soit le support utilisé. Elle peut aussi être utilisée pour l'échange sécurisé de fichiers sur un même réseau.

Note : La décontamination est effectuée sur le / les fichier(s) envoyé(s) mais n'est pas réalisée sur le média amovible.



3. Architecture Projet

3.1 Architecture globale



CyberHawk propose une architecture simple, décomposée en quatre zones physiques.



« Trusted Domain »

Domaine de confiance à sécurité renforcée sur lequel l'utilisation des médias amovibles doit être proscrite.

« Untrusted Domain »

Domaine à sécurité réduite ou non maîtrisé. Ce domaine permet un point d'entrée avec les médias amovibles. Il peut être composé de plusieurs postes et / ou de kiosques interactifs libre-service.



« DMZ »

Passerelle de sécurité entre les deux domaines précédents, la DMZ contient le serveur CyberHawk. Les fichiers échangés dans un sens comme dans l'autre transitent par ce serveur tout en étant décontaminés.



« Internet »

Le serveur Miroir permet la mise à jour quotidienne des signatures antivirales pour tous nos clients. Les mises à jour logicielles CyberHawk sont également mises à disposition pour une installation automatique et transparente !

Trois serveurs répartis dans trois domaines différents permettent le fonctionnement général du service et de la solution :



Serveur Principal CyberHawk

Ce serveur est composé d'un système Debian, d'un Firewall local et d'une sécurité renforcée. Il permet l'hébergement des services nécessaires à CyberHawk et propose une interface Web aux utilisateurs du service.



Serveur miroir

Ce serveur est composé d'un système Debian, d'un Firewall local et d'une sécurité renforcée. Il permet le stockage des mises-à-jour (Antivirus, Signatures Antivirales, Modules) après les avoir téléchargées sur les différents sites éditeurs. Les mises-à-jours sont ensuite packagées (conteneur chiffré) pour chaque client.



Serveur de mises-à-jour CyberHawk

*Ce serveur est composé d'un système Debian, d'un Firewall local et d'une sécurité renforcée. Il permet l'obtention des mises à jour CyberHawk (Antivirus, Signatures Antivirales, Code Source) depuis le **Serveur miroir**. Une fois téléchargées, les mises-à-jour sont envoyées vers le **Serveur Principal CyberHawk**.*

3.2 Echanges réseaux

Les échanges réseaux nécessaires à la solution CyberHawk ont été étudiés et conçus pour garantir une sécurité maximale des échanges :

- Empêcher la propagation de virus entre les deux domaines « **Trusted Domain** » et « **Untrusted Domain** ».
- Empêcher la propagation de virus potentiel en « **DMZ** ».
- Eviter toutes les connexions entrantes vers les différents domaines de nos clients afin de garantir une sécurité optimale.








				Miroir
		X	HTTP (TCP/80) HTTPS (TCP/443)	X
	X		HTTP (TCP/80) HTTPS (TCP/443) SSH (TCP/22)	HTTP (TCP/80)
	X	X		X
	X	X	X	

Table 1 - Matrice des flux réseaux autorisés entre domaines

3.3 Systèmes d'Exploitation

Tous les serveurs nécessaires à la solution CyberHawk sont installés sous une distribution Linux (Debian). Le choix de ce système d'exploitation a été motivé par le fait que les infections courantes sont souvent destinées à des systèmes Windows. De plus, ce système est jugé plus robuste face aux virus.

Au besoin, le **Serveur de mises-à-jour CyberHawk** peut être installé sur un système Windows. NÉOSOFT recommande néanmoins l'utilisation des systèmes de base.

3.4 Modules d'analyse

Trois moteurs antivirus sont utilisés par la solution.

NOM	LOGO	TARIF
ClamAV		Gratuit
Sophos		Gratuit
Comodo		Gratuit



Le choix des moteurs antivirus a été réalisé de sorte à ce que les antivirus CyberHawk soient différents et complémentaires à ceux couramment utilisés en entreprise.

Cette liste est susceptible d'évoluer en fonction des demandes et des évolutions futures. Les seules conditions requises à l'ajout d'un nouvel antivirus sont les suivantes :

- Fonctionnement de l'antivirus sur un système de type Linux
- Utilisation de l'antivirus en ligne de commandes

D'autres modules sont disponibles de base dans la solution et permettent l'analyse des fichiers envoyés :

- **Whitelist** : Permet de n'autoriser que certains types de fichiers ;
- **Blacklist** : Permet d'interdire certains types de fichiers ;
- **OCR (PDF)** : Permet d'autoriser ou d'interdire certains fichiers en fonction de leur contenu ;
- **OCR (Image)** : Permet d'autoriser ou d'interdire certains fichiers en fonction de leur contenu ;
- **VBA Blocker** : Permet de bloquer les documents Office contenant des macros VBA ;
- **Malicious VBA Blocker** : Permet de bloquer les documents Office contenant des macros VBA jugées malveillantes ;



4. Fonctionnement général

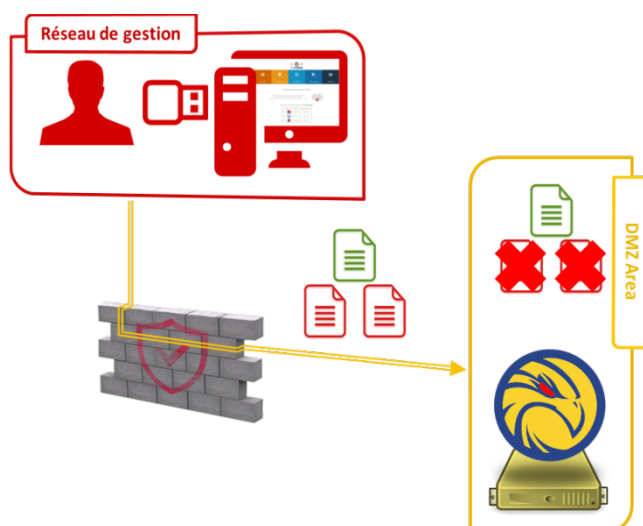
4.1 Envoi de fichiers depuis un media amovible

L'accès à l'interface de gestion de fichiers du **Serveur Principal CyberHawk** est réalisé en mode Web uniquement, à l'aide d'un navigateur web (Internet Explorer, Chrome, Firefox, etc.). L'interface est accessible à l'ensemble des utilisateurs créant un compte sur l'application (configuration possible afin de créer des comptes à la demande uniquement).

Si le choix d'un **Poste de Travail en Libre-Service** (ou kiosque interactif) est réalisé, seule l'Interface Web sera accessible et la navigation dans le système restera impossible.

Plusieurs états sont disponibles sur l'interface web du **Serveur Principal CyberHawk**. Des indicateurs visibles par tous les utilisateurs permettent de comprendre l'état de la plateforme (sous forme de drapeau) :

- **Vert** : Fonctionnement normal de l'application.
- **Orange** : Dysfonctionnement non bloquant. Utilisation de l'application possible mais non recommandée en raison d'un manque de mises-à-jour des bases de signatures antivirus. L'envoi et le téléchargement de fichiers restent néanmoins possibles.
- **Rouge** : Dysfonctionnement bloquant. Utilisation de l'application possible uniquement pour récupérer des fichiers déjà présents sur l'espace utilisateur. Envoi de fichiers impossible en raison d'un dysfonctionnement de l'un ou de plusieurs moteurs antivirus.

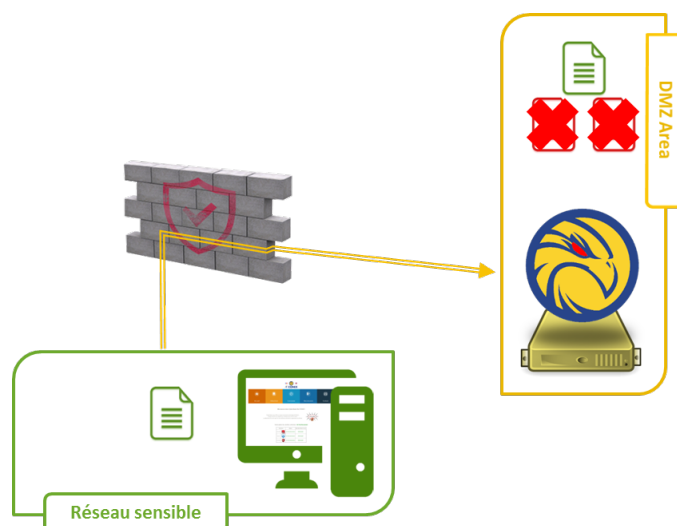


1. Le média amovible est inséré dans un Poste de Travail Libre-Service (ou, selon le choix client, sur un poste quelconque dans le réseau, kiosque interactif, etc.)



2. L'utilisateur, après s'être identifié / authentifié sur le portail web sur le **Serveur Principal CyberHawk**, envoie un ou plusieurs fichiers dans son espace personnel.
3. Le fichier est analysé par le **Serveur Principal CyberHawk** et supprimé dans le cas où il serait infecté. Dans le cas contraire, il est laissé à disposition de l'utilisateur dans son espace personnel

4.2 Récupération de fichiers depuis l'espace personnel



1. L'utilisateur, après s'être authentifié sur le portail web du **Serveur Principal CyberHawk**, récupère un ou plusieurs fichiers dans son espace personnel.



5. Mises-à-jour

5.1 Préambule

Lors de l'ajout d'un nouveau client sur le **Serveur miroir**, plusieurs informations sont générées automatiquement :

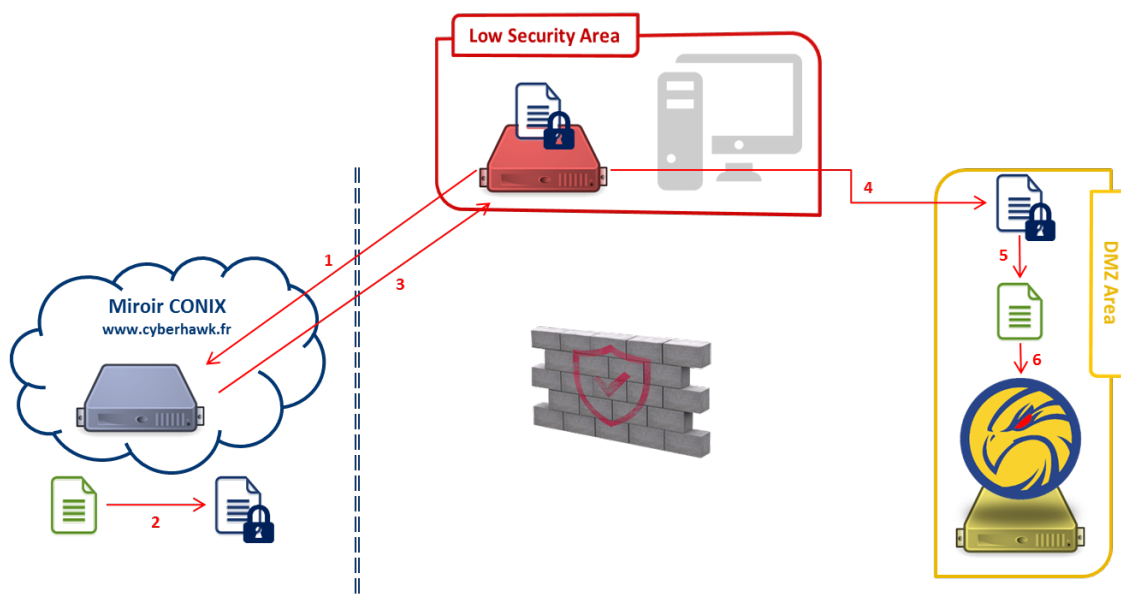
- Un identifiant client unique, lui permettant de venir télécharger automatiquement ou manuellement ses mises-à-jour sur le **Serveur miroir** (exemple : XXXX-XXXX-XXXX-XXXX-XXXX).
- Une clé de chiffrement unique, permettant d'envoyer les mises-à-jour chiffrées de bout en bout entre le **Serveur miroir** et le **Serveur Principal CyberHawk** (exemple : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX).

La clé de chiffrement est donc à renseigner lors de l'installation du **Serveur Principal CyberHawk**.

Le **Serveur de mises-à-jour CyberHawk** n'a aucune connaissance du contenu du fichier téléchargé et n'est pas en mesure de le déchiffrer.



5.2 Signatures Antivirales



1. Le **Serveur de mises-à-jour CyberHawk** envoie une requête quotidienne (incluant l'identifiant client unique) vers le **Serveur miroir** afin de récupérer les mises-à-jour de signatures antivirales.
2. Le **Serveur miroir** crée un conteneur chiffré (avec la clé de chiffrement unique) incluant les mises-à-jour de signatures antivirales.
3. Le **Serveur miroir** répond au **Serveur de mises-à-jour CyberHawk** en lui retournant le conteneur chiffré.
4. Le **Serveur de mises-à-jour CyberHawk** envoie le conteneur chiffré vers le **Serveur Principal CyberHawk** en SSH.
5. Le **Serveur Principal CyberHawk** déchiffre le conteneur et vérifie l'intégrité des mises-à-jour.
6. Le **Serveur Principal CyberHawk** installe les mises-à-jour sur le système.

5.3 Antivirus

Les mises-à-jour des moteurs antivirus sont réalisées de la même manière que les mises-à-jour des signatures antivirales.

La différence réside uniquement dans la périodicité de ces mises-à-jour qui ne sont plus quotidiennes mais sur demande / avec accord du client.



5.4 Code Source CyberHawk

Les mises-à-jour du code source CyberHawk sont réalisées de la même manière que les mises-à-jour des signatures antivirales.

La différence réside uniquement dans la périodicité de ces mises-à-jour qui ne sont plus quotidiennes mais à périodicité inconnue. Ces mises-à-jour seront effectuées avec l'accord préalable du client, à chaque fois qu'une nouvelle version stable du code source CyberHawk sera disponible.

5.5 Système d'Exploitations CyberHawk (Offline)

La mise-à-jour du système d'exploitation du **Serveur Principal CyberHawk** sera réalisée en mode hors-ligne (utilitaire APT-Offline) à la demande du client ou, à défaut, 2 fois par an maximum (sauf découverte de vulnérabilité critique affectant le système installé), tel que prévu par le contrat de maintenance.



6. Gestion des logs

6.1 Logs Serveur Principal CyberHawk

Les logs du **Serveur Principal CyberHawk** sont décomposés en deux grandes parties :

- Les logs de mises-à-jour
- Les logs d'utilisation de l'application CyberHawk

Détails concernant les logs de mises-à-jour :

- Date / Heure pour chaque entrée de log
- Requête SSH reçue depuis le **Serveur de mises-à-jour CyberHawk**
- Etat de la mise-à-jour (succès, échecs)
- Fichier(s) mis-à-jour

Détails concernant les logs d'utilisation de l'application CyberHawk :

- Date / Heure pour chaque entrée de log
- Actions d'authentification ou d'identification (Succès, Echec)
- Actions d'envoi de fichiers (logs de fichiers sains et de virus détectés avec MD5, SHA-1 et détails du virus).
- Actions de téléchargements de fichiers
- Actions de gestions d'utilisateurs (réalisables par l'administrateur uniquement).

Les logs d'utilisation de l'application CyberHawk sont disponibles sous deux formats :

- MySQL (Export XML possible)
- Syslog

6.2 Logs serveur de mises-à-jour CyberHawk

Les logs du **Serveur de mises-à-jour CyberHawk** sont minimalistes et contiennent uniquement les informations suivantes :

- Date / Heure pour chaque entrée de log
- Requête HTTP envoyée vers le **Serveur miroir**
- Réponse HTTP reçue du **Serveur miroir**
- Requête SSH envoyée vers le **Serveur Principal CyberHawk**



6.3 Logs miroir

Les logs du **Serveur miroir** contiennent les informations suivantes :

- Date / Heure pour chaque entrée de log
- Requête HTTP envoyée vers chaque site éditeur AV
- Réponse HTTP reçue depuis chaque site éditeur AV
- Requête HTTP reçue du **Serveur miroir**
- Informations relative à la création du conteneur chiffré
- Réponse HTTP envoyée vers le **Serveur miroir**