Functional Documentation

CYBERHAWK

FUNCTIONAL DOCUMENTATION

TABLE OF CONTENTS

1. Introduction

1.1 Definitions

ANTIVIRUS Antivirus is software designed to identify, neutralize and eliminate malicious software (including computer viruses).

ENCRYPTION Encryption is a cryptographic process by which it is desired to make the comprehension of a document impossible for anyone who does not have the (de)encryption key.

CYBERHAWK NÉOSOFT decontamination solution

DEBIAN Debian GNU / Linux is a specific distribution of the Linux operating system including many packages.

FIREWALL A Firewall is software and / or hardware to enforce the network security policy, which defines the types of communications allowed on that network. It measures the prevention of applications and packages.

LOG The “log” term represents an event history and, by extension, the file containing this history.

SAS A SAS is a mean that allows passing from one place to another, from one environment to another.

1.2 Abbreviations

APT	Advanced Package Tool
AV	Antivirus
DMZ	DeMilitarized Zone
FW	Firewall
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IS	Information System
MD5	Message Digest 5
SHA-1	Secure Hash Algorithm 1
SSH	Secure Shell
TCP	Transmission Control Protocol
USB	Universal Serial Bus

2. Overview

In order to transfer files (firmware, documents etc.) from removable media (USB drives) to trusted / sensitive networks, physical interventions on network equipment(s) are required.

Inherent problematic with this practice is spreading (automatically or not) potentially malicious elements inside the trusted / sensitive network. These elements, according to their threat level, could affect the availability, integrity or confidentiality of the network.

The NÉOSOFT "CyberHawk" solution eliminates the need of removable media usage inside trusted / sensitive network, using modules decontamination on an isolated server, accessible via a web interface for file transfers.

Access to the file management web interface can be provided on a separated information system (IS), or on a secure dedicated station (self-service / kiosk station).

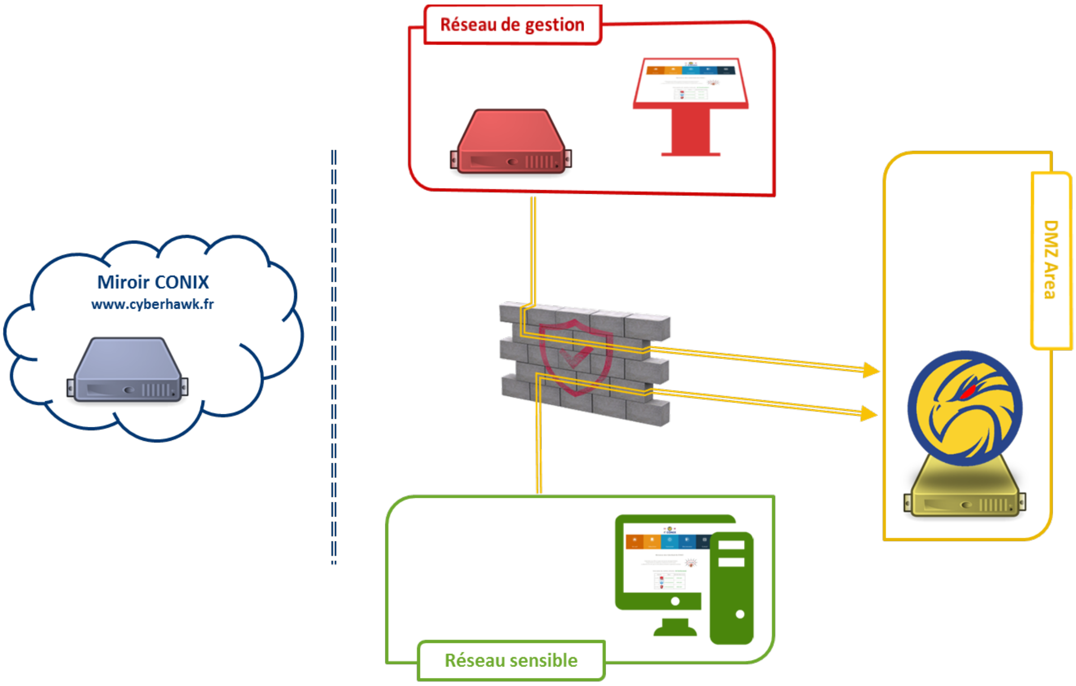
Within CyberHawk, each user is free to create his personal space and transfer files of their choice. These files are then analyzed by several modules (antivirus engines, scripts, blacklists, etc.) before being stored (or deleted if a threat is detected by at least one antivirus).

Unlike competitive solutions allowing USB keys decontamination on physical terminal, CyberHawk allows decontamination via the network, regardless of the medium used. It can also be used for secure files’ exchange on the same network.

Note: Decontamination is performed on the sent file(s) but is not performed on the removable media.

3. Project Architecture

3.1 Overall Architecture



CyberHawk offers a simple architecture, split into four physical areas.

« Trusted Domain »

Trusted domain with enhanced security on which the use of removable media should be prohibited.

« Untrusted Domain »

Reduced or uncontrolled security domain. This domain allows an entry point for removable media. It can be composed of several stations and / or self-service interactive kiosks.

« DMZ »

Security gateway between the two previous domains: the DMZ contains the CyberHawk server. The files exchanged in one direction or in the other transit through this server while being decontaminated.

« Internet »

Miroir CONIX
www.cyberhawk.fr

Your mirror allows the daily updating of antiviral signatures for all of our clients. CyberHawk software updates are also available for automatic and transparent installation!

Three servers distributed in three different domains allow the general operation of the application:

Main CyberHawk Server

This server is composed by a Debian system, a local firewall, and enhanced security. It provides hosting services for CyberHawk and provides a web interface for users of the service.

Mirror Server

This server is composed by a Debian system, a local firewall, and enhanced security. It allows the updates storage (Antivirus, Antiviral Signatures) after their download on editors' websites. The updates are then packaged (encrypted container) for each customer.

CyberHawk Update Server

*This server is composed by a Debian system, a local firewall, and enhanced security. It allows client to download CyberHawk updates (Antivirus, Antiviral Signatures and Source Code) from **Mirror Server**. Once downloaded, updates are sent to **Main CyberHawk Server**.*

3.2 Network Exchanges

Network exchanges required for the CyberHawk solution were studied and designed to guarantee maximum security:

- Prevent the spread of viruses between the two domains ***« Trusted Domain »*** and ***« Untrusted Domain »***.
- Prevent the spread of potential viruses within the *« DMZ »*.
- Avoid all incoming connections to the different domains of our customers in order to guarantee an optimal security.

	Réseau sensible	Réseau de gestion	DMZ	Mirror
Réseau sensible	╳	X	HTTP (TCP/80) HTTPS (TCP/443)	X
Réseau de gestion	X	╳	HTTP (TCP/80) HTTPS (TCP/443) SSH (TCP/22)	HTTP (TCP/80)
DMZ	X	X	╳	X
Miroir CONIX www.cyberhawk.fr	X	X	X	╳

Table 1 - Matrix of authorized network flows between domains

3.3 Operating Systems

All servers required by CyberHawk solution are installed under a Linux (Debian) distribution. The choice of this operating system was motivated by the fact that common infections are often intended for Windows systems. In addition, this system is considered more robust against viruses.

If necessary, the ***CyberHawk Update Server*** can be installed on a Windows system. However, NÉOSOFT recommends the use of basic systems.

3.4 Analysis plugins

Three antivirus engines are used by the solution.

NAME	LOGO	PRICE
ClamAV	ClamAV	Free
Sophos	S	Free
Comodo	C	Free

The choice of CyberHawk antiviral engines has been made to ensure difference and complementary with those commonly used in companies.

This list is likely to evolve in response to future demands and developments. The only requirements for adding a new antivirus are as followings:

- Compatibility of the antivirus with Linux systems
- Usage of antivirus possible in command line

Other plugins are made available within solution allowing analysis of uploaded files:

- ***Whitelist*** : Allow only a file list based on their mime type ;
- ***Blacklist*** : Disallow a file list based on their mime type ;
- ***OCR (PDF)*** : Allow or disallow some files based on their content ;
- ***OCR (Image)*** : Allow or disallow some files based on their content ;
- ***VBA Blocker*** : Block Office documents including VBA macros ;
- ***Malicious VBA Blocker*** : Block Office documents including potentially malicious VBA macros ;

4. General functioning

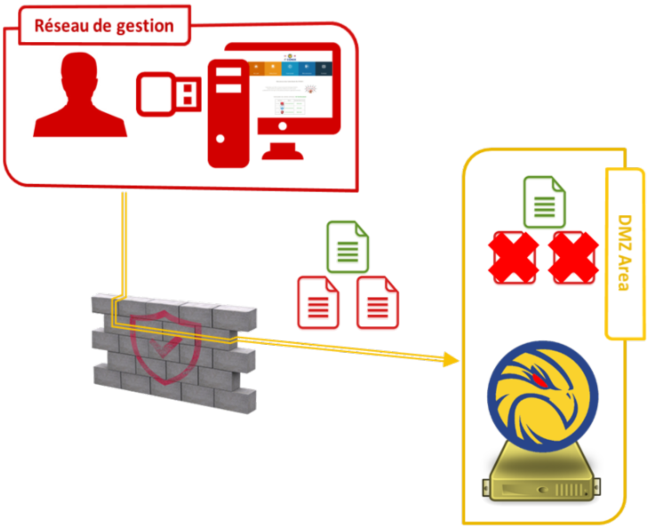
4.1 Sending files from removable media

Access to file management interface of the Main CyberHawk Server is realized in Web mode only, using a web browser (Internet Explorer, Chrome, Firefox, etc.). This interface is available to all users having an account on the application (configuration possible to create accounts on request only).

On **Self-Service Station**, only the Web Interface is accessible and the system access is made impossible.

Several states are available on the Main CyberHawk Server web interface. Indicators are made available to all users for viewing the state of the platform (flags):

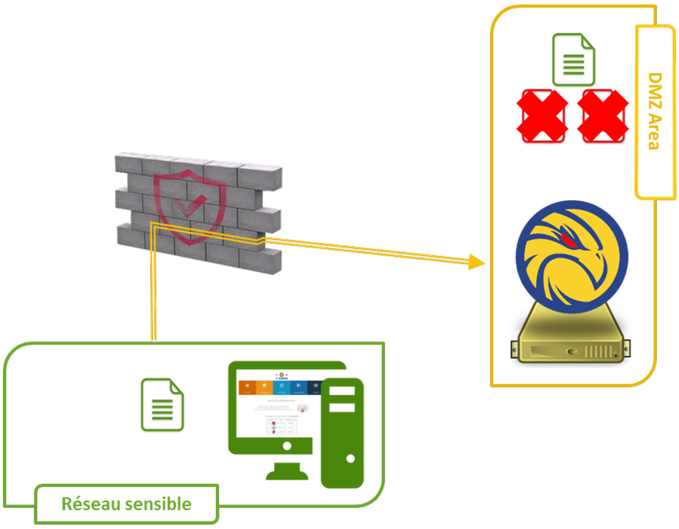
- Green: Application in normal operating mode.
- Orange: Non-blocking malfunction. Using the application is possible, but not recommended due to a lack of antivirus signature databases update. Uploading and downloading files remain possible.
- Red: Blocking malfunction. Using the application is possible for downloading files already present within the user's space. Files' upload is not possible due to a malfunction of one or more antivirus engines.



1. Removable media is inserted within **Self-Service Station** (or, depending on customer's choice, on any station within "untrusted" domain).
2. User, after being identified / authenticated on the Main CyberHawk Server's web interface, uploads one or more file to his personal space

3. File is then analyzed by the Main CyberHawk Server and removed if a potential threat is detected. Otherwise, it is left available to the user in his personal space.

4.2 Downloading files from personal space



1. User, after being identified / authenticated on the Main CyberHawk Server's web interface, downloads one or more file from his personal space.

5. Updates

5.1 Preamble

When adding a new client to the **Mirror Server**, several information is generated automatically:

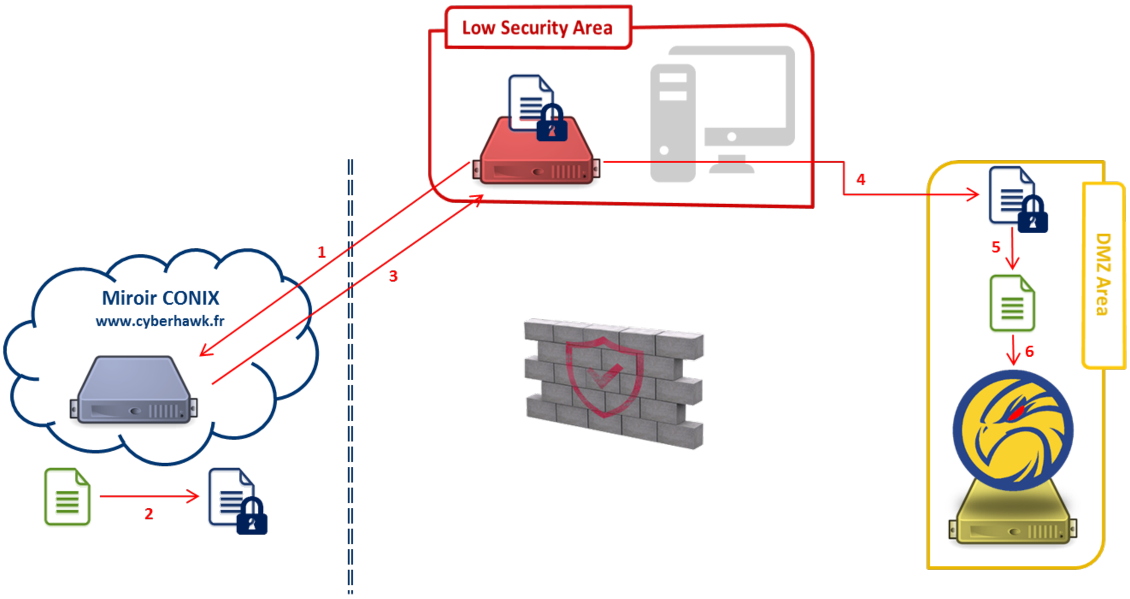
- A unique client identifier, allowing to download updates automatically or manual from **Mirror Server** (example: XXXX-XXXX-XXXX-XXXX-XXXX).

- A unique encryption key, allowing to send end-to-end cyphered updates between the **Mirror Server** and the **Main CyberHawk Server** (example: XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX).

  The encryption key is to be filled in when installing the **Main CyberHawk Server**.

  The ***CyberHawk Update Server*** has no knowledge of the contents of the downloaded file and is not able to decipher it.

5.1 Antiviral Signatures



1. The **CyberHawk Update Server** sends a daily query (including the unique client identifier) to the **Mirror Server** to retrieve antivirus signature updates.
2. The **Mirror Server** creates an encrypted container (with the unique encryption key) including antivirus signature updates.
3. The **Mirror Server** answers to **CyberHawk Update Server** request by returning the encrypted container file.
4. The **CyberHawk Update Server** sends the encrypted container to the Main CyberHawk Server using SSH.
5. The Main CyberHawk Server decrypts the container and verifies the integrity of the updates.
6. The Main CyberHawk Server installs updates on the system.

5.2 Antivirus

Antiviral engine updates are performed in the same way as antiviral signatures updates.

The difference is only the periodicity of these updates which are no longer daily but on demand / agreement with the client.

5.3 CyberHawk source code

The CyberHawk source code updates are performed in the same way as antiviral signatures updates.

The difference is only the periodicity of these updates which are no longer daily but on unknown periodicity. These updates will be done with the prior agreement of the customer, whenever a new stable version of the CyberHawk source code will be available.

5.4 CyberHawk Operating Systems (Offline)

Operating System update for **Main CyberHawk Server** will be made offline (APT-Offline package) on client request or, by default, twice a year maximum (unless discovery of critical vulnerability affecting the installed system), as planed within the maintenance contract.

6. Logs management

6.1 Main CyberHawk Server Logs

Logs of Main CyberHawk Server are split in two main parts:

- Updates logs
- CyberHawk application usage logs

Update logs' details:

- Date / Time for each log entry
- SSH request received from **CyberHawk Update Server**
- Update state (success, failure)
- Updated file(s)

CyberHawk application usage logs' details:

- Date / Time for each log entry
- Authentication or Identification actions (Success, Failure)
- Files sent (log of safe and unsafe files with MD5, SHA-1 and details about the virus).
- Files downloaded
- Users' management actions (only available for administrator).

CyberHawk application usage logs' details are available in two formats:

- MySQL (XML file export)
- Syslog

6.2 CyberHawk Update Server Logs

Logs of **CyberHawk Update Server** are minimalist and contain only the following information:

- Date / Time for each log entry
- HTTP request sent to **Mirror Server**
- HTTP reply received from **Mirror Server**
- SSH request sent to **Main CyberHawk Server**

6.3 Mirror Server Logs

Logs of **Mirror Server** contain the following information:

- Date / Time for each log entry
- HTTP request sent to each AV editor’s website
- HTTP reply received from each AV editor’s website
- HTTP request received from **Mirror Server**
- Information related to cyphered container creation
- HTTP response sent to **Mirror Server**