

# Cyber47&Moi

## Table des matières

Cyber47&Moi .....	1
Actions effectuées : .....	1
Démarrage .....	2
Procédures .....	3
Verrouillage PC et utilisateur .....	3
Génération du code pour réactiver les connexions réseaux .....	5

Le programme se situe sous O:\Techs\outiladmins\outiladmins.exe

### Actions effectuées :

- Suppression de l'utilisateur du groupe VPN\_F5\_UTIL
- Suppression de l'utilisateur du groupe VPN\_F5\_DSIAN
- Suppression de l'utilisateur du groupe VPN\_F5\_VIP
- Suppression de l'utilisateur du groupe F5\_ACTIVESYNC\_2010
- Désactivation du compte utilisateur
- Changement du mot de passe du compte utilisateur
- Désactivation du compte ordinateur
- Suppression de l'ordinateur du groupe GPO\_VPN\_F5\_O

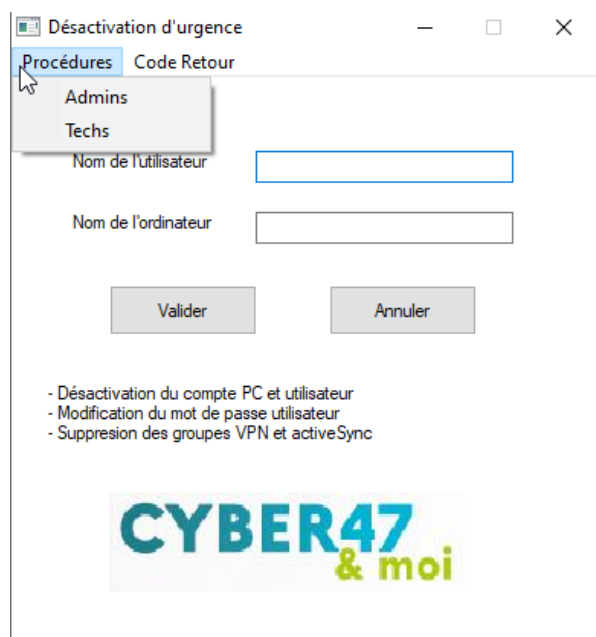
## Démarrage



Cliquer sur le logo **Cyber47&moi**

## Procédures

Les procédures d'urgence des administrateurs et des Techniciens sont disponibles via le menu « Procédures »



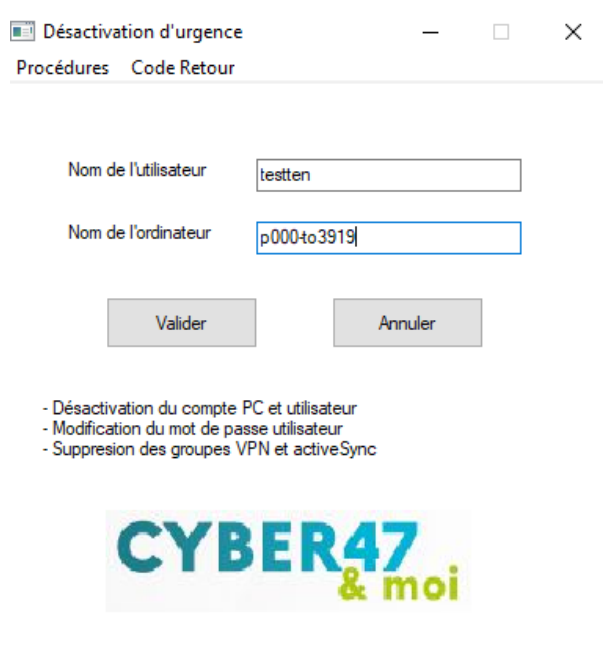
The screenshot shows a window titled 'Désactivation d'urgence' with a standard Windows interface (minimize, maximize, close buttons). Inside the window, there are two tabs: 'Procédures' (selected) and 'Code Retour'. Under the 'Procédures' tab, there is a dropdown menu with two options: 'Admins' and 'Techs'. Below the menu, there are two text input fields: 'Nom de l'utilisateur' and 'Nom de l'ordinateur'. At the bottom of the form area, there are two buttons: 'Valider' and 'Annuler'. Below the buttons, there is a list of actions to be performed:

- Désactivation du compte PC et utilisateur
- Modification du mot de passe utilisateur
- Suppression des groupes VPN et activeSync

At the very bottom of the window, there is a logo that reads 'CYBER47 & moi'.

## Verrouillage PC et utilisateur

*Lorsqu'un utilisateur a déclenché l'alerte Cyber ou soupçonne une attaque Cyber, nous devons lui retirer des droits et désactiver les comptes Utilisateur et Ordinateur, en effectuant la « **Désactivation d'urgence** » avec la grille suivante :*



This screenshot shows the same 'Désactivation d'urgence' window, but now the input fields are populated. The 'Nom de l'utilisateur' field contains the text 'testten' and the 'Nom de l'ordinateur' field contains the text 'p000to3919'. The 'Valider' and 'Annuler' buttons remain at the bottom, along with the list of actions and the 'CYBER47 & moi' logo.

Après avoir saisi le nom de l'utilisateur et son nom d'ordinateur, le bouton « Valider » effectue toutes les tâches qui sont affichées :

mot de passe X

Le mot de passe pour 'testten' a été changé

OK

Gestion des groupes X



Supression du groupe VPN\_F5\_UTIL effectuée

OK

Gestion des groupes X



Supression du groupe F5\_ACTIVESYNC\_2010 effectuée

OK

Gestion de l'utilisateur X



L'utilisateur 'testten' est désactivé

OK

Gestion du PC X



Le PC 'p000-to39195' est désactivé

OK

Gestion des groupes X



Suppression du groupe GPO\_VPN\_F5\_O effectuée

OK

Puis, affichage d'une fenêtre donnant tous les groupes dont l'utilisateur est encore membre :



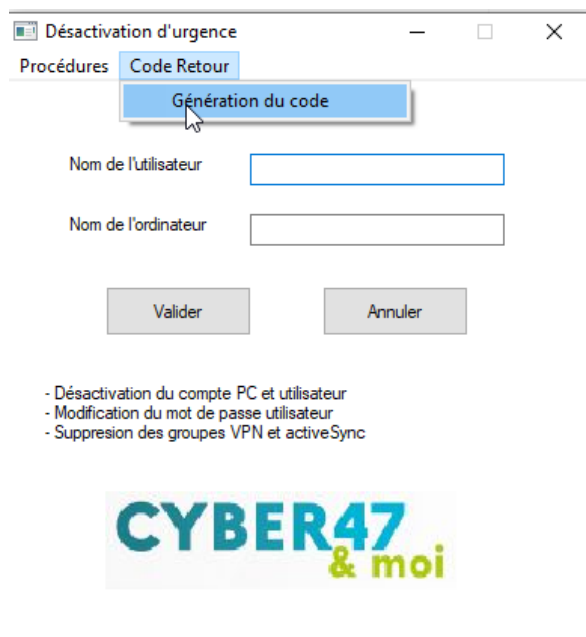
Un log retraçant toutes les opérations effectuées est créé sous :

« K:\Reseau\0-Admin&Tech\Utilisateurs\Trace Cyber ».

### Génération du code pour réactiver les connexions réseaux

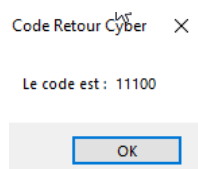
*Lorsqu'un utilisateur a déclenché l'alerte Cyber, toutes les cartes réseaux sont désactivées. Après avoir effectué tous les contrôles et actions nécessaires, nous devons réactiver les comptes Utilisateur et Ordinateur et remettre les droits retirés.*

*A l'exécution du programme « C:\Program Files\DSIAN\RetourCyber.exe » permettant de réactiver les cartes réseau, un code est demandé (suivre procédure ci-dessous pour l'obtenir).*



The screenshot shows a window titled "Désactivation d'urgence" with a tabbed interface. The "Code Retour" tab is selected, and within it, the "Génération du code" sub-tab is active. Below the tabs, there are two input fields: "Nom de l'utilisateur" and "Nom de l'ordinateur". Below these fields are two buttons: "Valider" and "Annuler". At the bottom of the window, there is a list of actions: "- Désactivation du compte PC et utilisateur", "- Modification du mot de passe utilisateur", and "- Suppression des groupes VPN et activeSync". At the very bottom, there is a logo that reads "CYBER47 & moi".

La tâche « Génération du code » du menu « Code Retour » génère le mot de passe pour réactiver les cartes réseau d'un PC utilisateur ayant déclenché l'alerte Cyber.



The screenshot shows a small dialog box titled "Code Retour Cyber". Inside the dialog, it says "Le code est : 11100". At the bottom of the dialog, there is an "OK" button.