Red Plan

Go to this plan if you suspect the red team is on your system. Keep in mind these methods are merely a guide and not a step-by-step process. You may return to green plan at your own risk.

1. Logoff Bad Users and Change User Passwords

```
C:\> query user

    Keep note of the ID associated with each connection

C:\> logoff <<ID NUMBER>>

C:\> for /F %i in ('wmic UserAccount get name') do @net
    user %i <<NEW PASSWORD>>

    Close the CMD and re-open to clear history
```

2. Disconnect Bad SMB Sessions

```
    View outbound sessions
C:\> net use

    Disconnect sessions
C:\> net use \\<<IP ADDRESS>> /del /y

    View inbound sessions (be careful with these)
C:\> net session

    Disconnect sessions
C:\> net session \\<<IP ADDRESS>> /del
```

3. Bad Users and Groups Configurations

```
        View users
C:\> net user

        Delete (not disable) bad users
C:\> net user <<USERNAME>> /delete

        View users in sensitive groups
C:\> net localgroup Administrators
C:\> net localgroup “Remote Desktop Users”

        Remove unauthorized users from a group
C:\> net localgroup <<GROUP>> <<USER>> /delete
```

4. Terminate Bad Processes

```
        Kill a bad process (by name)
C:\> wmic process where name=”<<PROCESS>>” delete

        Kill a process by PID
C:\> wmic process where processid=”<<PID>>” delete
```

5. Credential User Interface (Gpedit.msc)

a. Computer Configuration > Administrative Templates > Windows Components > Credential User Interface

This requires you to type a password every time you want to elevate.

6. Block an IP Address

If you are ABSOLUTELY sure that the only way to get the red team out is to block an IP address…

```
C:\> netsh advfirewall firewall add rule name="BLOCK RED
     TEAM" dir=in protocol=tcp localport=any action=block
     remoteip=<<IP YOU WANT TO BLOCK>>
```

Note that the IP won't actually be blocked until it re-connects. Any current connections won't be kicked.