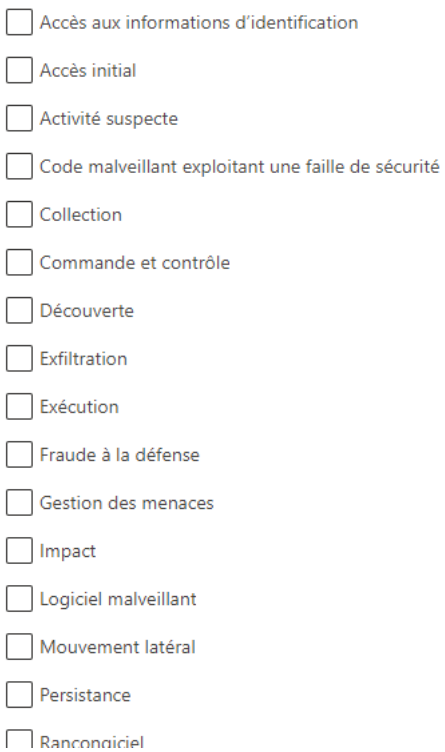
DEBLOCAGE DE COMPTE O365

I. SOMMAIRE

II. CAUSES DE BLOCAGE

Dans notre entreprise, les comptes Microsoft peuvent se bloquer automatiquement pour des raisons de sécurité. Ce blocage peut intervenir pour différentes raisons. A notre niveau, en tant que technicien support nous gérons principalement des compte bloqué du à trop d'erreur de tentatives de connexion ou un changement de localisation du à notre Proxy . Pour visualisé la liste des Alertes , nous allons sur notre portail d'administration Exchange

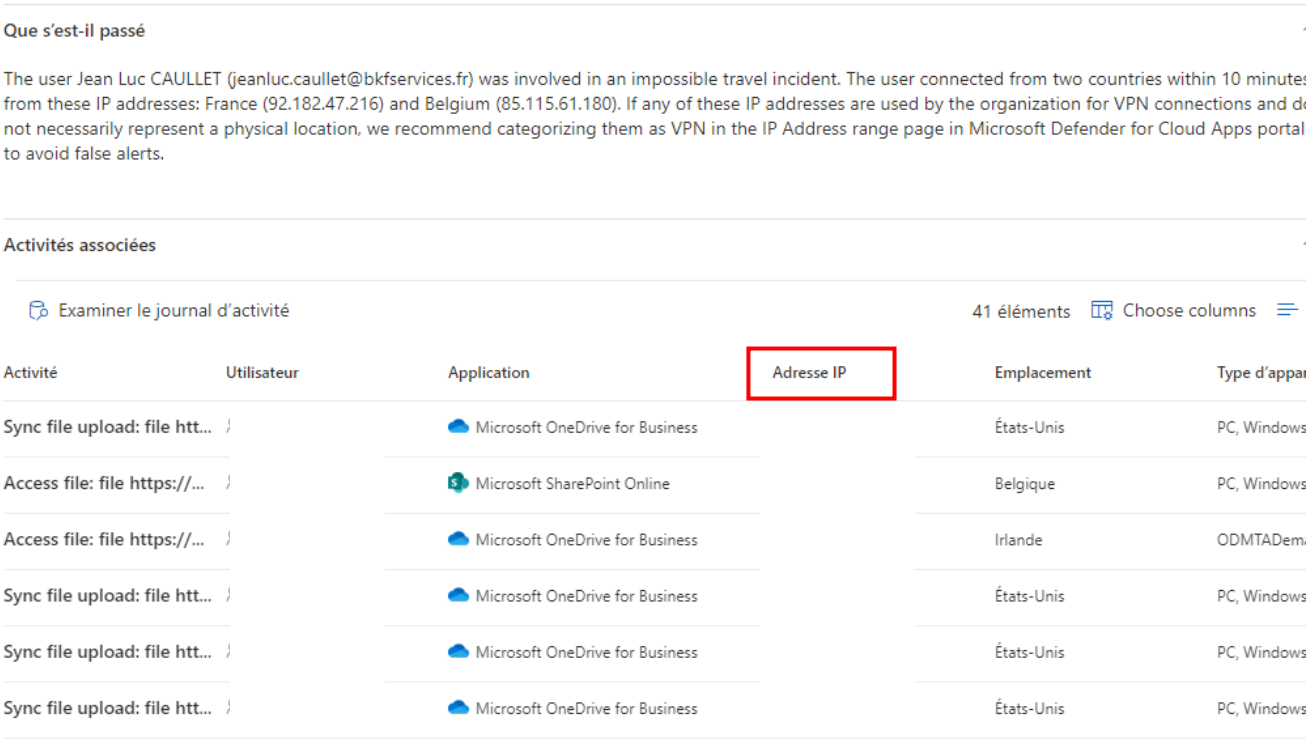


III. TENTATIVES DE CONNEXION INCORRECTE EXCECIVES

Si un trop grand nombre de tentative échoué est détecté par Microsoft, le compte peut être bloque automatiquement. Voici un exemple :

IV. CHANGEMENT D'ADRESSE IP PAR FORCEPOINT

Parfois, en raison d'une surcharge sur les serveurs français, notre proxy ForcePoint peut transférer un compte vers des serveurs situés en Belgique, aux États-Unis ou au Luxembourg. Ce déplacement entraîne un changement d'adresse IP, ce qui est interprété par Microsoft comme un déplacement géographique rapide, déclenchant ainsi le blocage du compte. Voici un exemple. (Certains détails sont cachés pour des raisons de confidentialités)



Que s'est-il passé

The user Jean Luc CAULLET (jeanluc.caullet@bkfservices.fr) was involved in an impossible travel incident. The user connected from two countries within 10 minutes from these IP addresses: France (92.182.47.216) and Belgium (85.115.61.180). If any of these IP addresses are used by the organization for VPN connections and do not necessarily represent a physical location, we recommend categorizing them as VPN in the IP Address range page in Microsoft Defender for Cloud Apps portal to avoid false alerts.

Activités associées

Examiner le journal d'activité — 41 éléments — Choose columns

Activité	Utilisateur	Application	Adresse IP	Emplacement	Type d'appar
Sync file upload: file htt...		Microsoft OneDrive for Business		États-Unis	PC, Windows
Access file: file https://...		Microsoft SharePoint Online		Belgique	PC, Windows
Access file: file https://...		Microsoft OneDrive for Business		Irlande	ODMTADem
Sync file upload: file htt...		Microsoft OneDrive for Business		États-Unis	PC, Windows
Sync file upload: file htt...		Microsoft OneDrive for Business		États-Unis	PC, Windows
Sync file upload: file htt...		Microsoft OneDrive for Business		États-Unis	PC, Windows

Ici, nous pouvons voir que son emplacement change fréquemment du à notre Proxy .

V. PROCEDURE DE DEBLOCAGE

Avant de débloquer un compte, nous procédons comme suit :

- Consultation des alertes : Nous consultons le suivi des alertes qui répertorie tous les comptes bloqués automatiquement. Ce suivi nous permet de comprendre la raison du blocage.

- Analyse : Si l'alerte indique, par exemple, que l'adresse IP a été modifiée par ForcePoint, nous savons que le changement est légitime. Dans ce cas, le compte peut être débloqué en toute sécurité. Nous classons l'alerte comme "résolu" par la suite

- Déblocage : Le compte doit être alors débloqué directement via le portail d'administration Office ou Azure AD.

VI. EN CAS D'ACTIVITE SUSPECTE

Si une activité suspecte en gravité élevée est détectée, plutôt que de débloquer le compte nous-même, nous prévenons notre équipe Infrastructure. Ils sont chargés d'analyser la situation plus en détail avant toute action sur le compte.