Suspicious Sign Ins

https://campus.barracuda.com/doc/86541493/

For important information about suspicious sign-in data and your environment, refer to Getting Started.

Before You Begin

Before Impersonation Protection can collect sign-in data, you must turn on the Microsoft audit log search. To turn on Microsoft audit log search, read and follow Microsoft's instructions.

Viewing Suspicious Sign Ins

To view suspicious sign ins:

1. Log into Impersonation Protection at https://sentinel.barracudanetworks.com/signin.
2. Click the menu button in the top left corner and select **Account Takeover Protection**. Then select the **Sign Ins** tab.
3. You can search for an email or account or view sign ins in a list by country or in a map. To view a suspicious sign in, click **View** or click a spot on the map.
4. The following information about suspicious activity displays for the account:
    - Date – Date and time of sign-in
    - Account – Account in your organization that was affected
    - IP of sign in – IP origin of the sign in
    - User Agent – Method used to access the account
    - Location – Country origin of the sign in
    - Status – Whether the hacker's login attempt was a success or a failure.

Click **View Related Sign Ins** to see related sign ins for that account.

Note that sign-in information is kept for 30 days. Related sign ins over 30 days are not visible.