Alert Logins from Users outside your City or Country

DLP (Data Loss Prevention) · https://gatlabs.com/knowledge/tech-tips/alert-logins-from-users-outside-your-city-or-country/

Introduction

In this post, we will cover how to set up an Alert Rule for logins of Google Cloud workers (end-users) outside your City or Country of work.

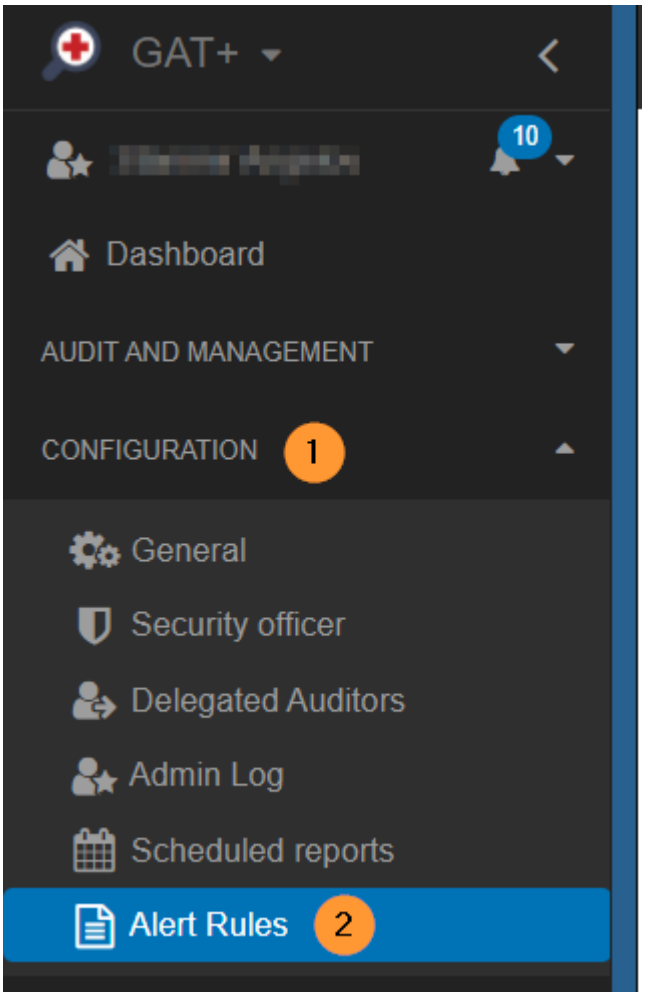
With remote work on the rise, organizations must learn to secure their users and enforce their policies on a continuous basis. GAT Labs facilitates just that, using a powerful Alert Rule notification feature.

This feature helps Google Workspace Super Admins to identify any compromised accounts in their Google Workplace.

Getting Started

To get started on setting up your Alert rule.

Navigate **GAT+ > Configuration > Alert Rules**



Add a new rule

Once in the '**Alert Rules**' section click on the **+ button** to set up a new "**User Logins**" alert.

You can also edit an existing one using the 'pen' icon.

Set the scope

You can set the **‘Scope’** to be either countries or cities.

We recommend starting with countries.

Enter a list of countries where you expect legitimate logins to occur, once the rule is saved it will begin execution.

School students, in particular, are very susceptible to these types of account thefts for several reasons for which,

- They tend not to have 2FA and to use their accounts or passwords on dubious sites.

- They might not even be aware that they are co-sharing their accounts with overseas individuals.

Check the status of compromised accounts

User Logins History

To see if any accounts have already been compromised you can go to the '**User Logins'** report area where you can filter for successful logins from outside your own country.

GAT+ > Audit & Management > Users Logins

How to find events?

Click on the Events tab in the top left corner.

Apply filter and search:

- Country not equal - select the country (the USA as an example)
- Event equal - select the event (OK as an example)

> When you have a list of suspicious accounts, do not jump to immediate conclusions. We recommend first checking with the account owner to see if they have been abroad on holiday or if there is some other legitimate reason for an overseas login.

We hope this new feature will help increase your domain security and alert you to potential dangers.

Video how-to

Embedded media:

https://www.youtube.com/embed/AsYQyykF_lQ?feature=oembed&color=red&rel=0&controls=1&start=&end=&fs=0&iv_loa