Template - Mail redirect via ExO transport rule

Link to alert

**Description**

Identifies when Exchange Online transport rule configured to forward emails. This could be an adversary mailbox configured to collect mail from multiple user accounts.

Do not bypass filtering for all internal messages; in this situation, a compromised account could send malicious content.

**Alert details**

Date:

User:

Email Redirect To:

Client IP:

Port:

Operation:

Rule Name:

**Remediation**

Confirm if the Transport rule to bypass EOP and allow mail to flow without delay from internal senders such as scanners, faxes, and other trusted sources that send attachments that are known to be safe. If IT Support did not create the mailflow rule, ensure that it is removed

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***