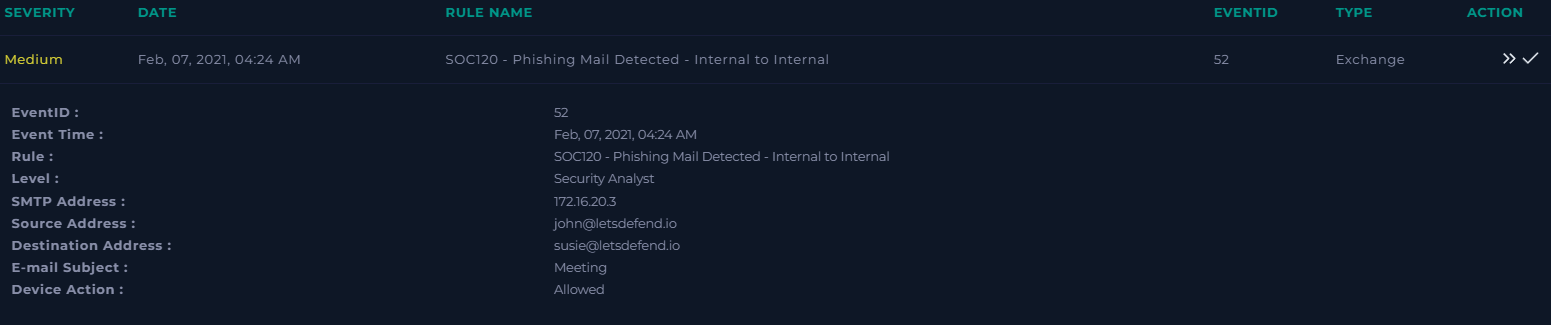
In this activity, I will investigate the ‘SOC120 - Phishing Mail Detected - Internal to Internal’ alert from letsdefend.



When creating the playbook for this alert first I gather general information about the alert.

When was it sent?

The email was sent at 04:24 AM on February 07, 2021.

What is the email's SMTP address?

The emailer's SMTP address is 172.16.20.3.

What is the sender address?

The sender’s address is john@letsdefend.io.

What is the recipient address?

The recipient’s address is [susie@letsdefend.io](mailto:susie@letsdefend.io).

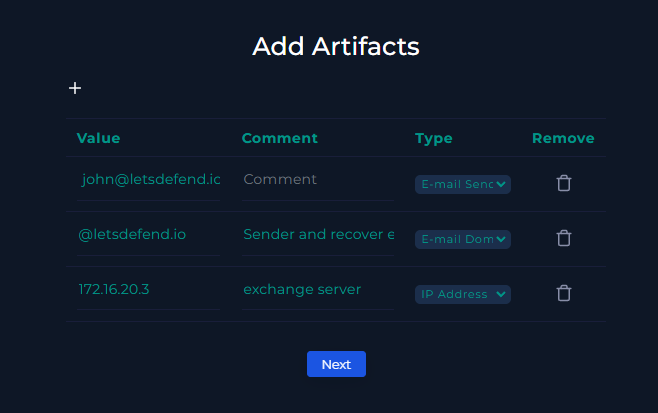
As the device action is ‘allowed’, we know that the mail reached the user.

Searching the email security, I found the contents of the sent email.



Is the mail content suspicious?

This email isn’t suspicious as it is sent from two users @letsdefend. Also it can’t be a phishing attack as it contains no links or attachments.



Analysis note:

This is not a phishing email.