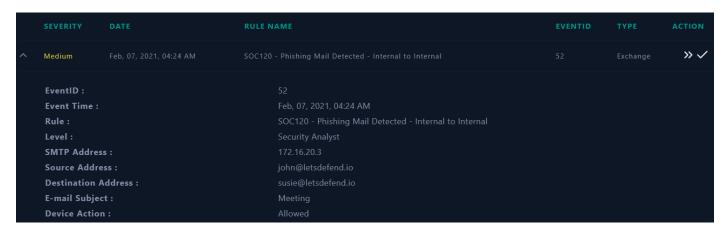
SOC120 - Phishing Mail Detected - Internal to Internal



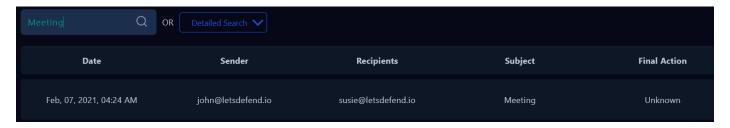
Click on >> and create case and click Continue.

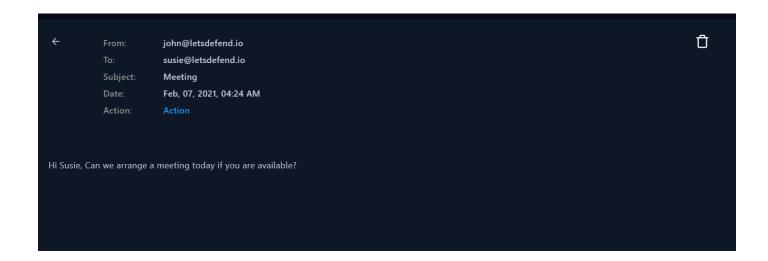


Let's check what info we have with us currently before we start with the Playbook.

The rule says, "Phishing Mail Detected" ... so we start by taking a look at the mail to identify the contents.

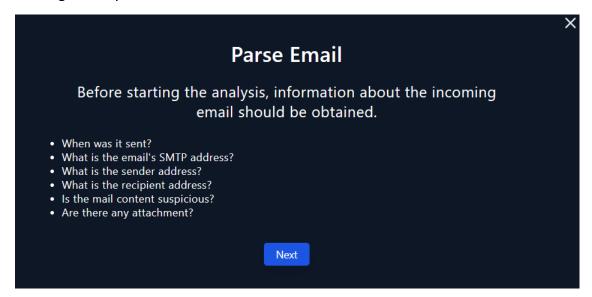
Click on Email Security and search for the mail with "Meeting" as mentioned in the alert.





Upon opening the email, we see that there is no attachment or links which rules out that there could be a malicious intent. The email is personalised towards the recipient and is an internal mail with the SMTP being a private IP address which clearly shows that this is an email exchange between two colleagues.

Starting the Playbook!



When was it sent? Feb, 07, 2021, 04:24 AM

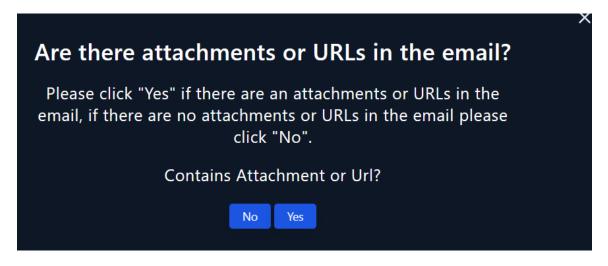
What is the email's SMTP address? 172.16.20.3

What is the sender address? john@letsdefend.io

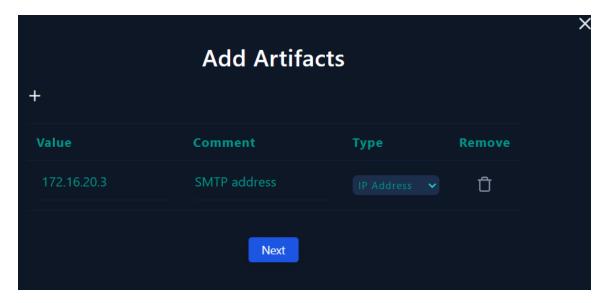
What is the recipient address? susie@letsdefend.io

Is the mail content suspicious? No

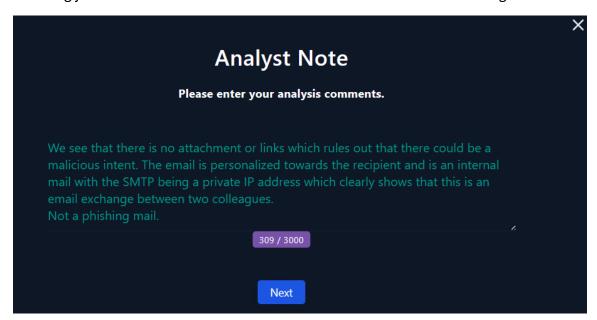
Are there any attachment? No



Selecting NO here.

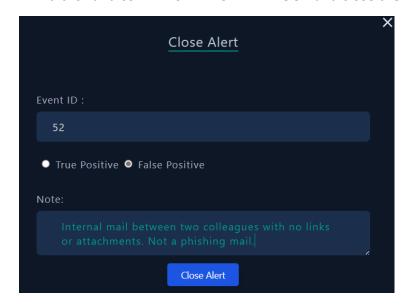


Selecting just the SMTP address as there are no other artifacts worth adding.



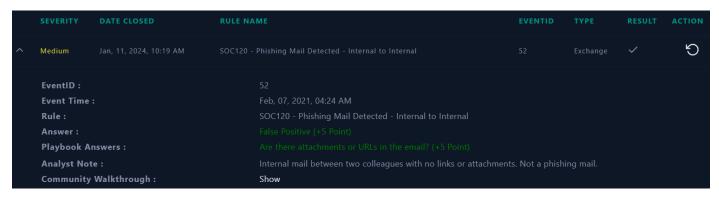
Not a Phishing Mail.

.. And click and confirm on FINISH PLAYBOOK and close the Alert.



Marking this as FALSE POSITIVE since the alert was generated for a Phishing Mail which it wasn't.

Let's check the scores now.



Hope this helped.