EventID 52 SOC120 Phishing Email Detected Internal to Internal

- Email was sent at: 2021, (Friday) 7th of February at 04:24h
- Destination address: 172.16.20.3:25
  - This is the SMTP Server that received the email
- Source address: 172.16.17.82:49582
- Email address of the sender: john@letsdefend.io
- Email address of the recipient: susie@letsdefend.io
- Subject: “Meeting”
- Device action: Allowed

This incident is of type “Exchange”, indicating that it’s related to Microsoft Exchange.

About the Email

As the title sugests, both the sender and recipient of the suspicious email come from “letsdefend.io” domain. This could indicate that:

- A legitimate account (john@letsdefend.io) has been compromised
- Or there’s unauthorized access to the internal SMTP Server

The email was sent at 4:24h in the morning, which doesn’t seem right because it’s outside of working hours.

After looking further into the email on the Email Security section of LetsDefend, the email:

- Doesn’t have any attachments
- Doesn’t provide any URLs
- The body of the email is not suspicious, just a regular request for a meeting

I’ve looked on Log Management for metadata of the email:

- The source and destination addresses come from the same private IP range (172.16.x.x). This means the source domain is not spoofed

By looking for the source address (172.16.17.82) at Endpoint Security, I’ve proved that the machine is legitimate, and no suspicious network activity is displayed.

Conclusion

The target email of this incident doesn’t look suspicious because there’s no attachments or URLs, and the email body is short and harmless.

The metadata of the email has been analyzed, proving that the source address comes from the same domain as the recipient.

This is a false positive, and the SIEM likely generated the alert based on behavioral analysis, because the email was sent outside of standard working hours (at 4:24 in the morning).