

SOC120 - Phishing Mail Detected - Internal to Internal

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
Medium	Feb, 07, 2021, 04:24 AM	SOC120 - Phishing Mail Detected - Internal to Internal	52	Exchange	>> ✓
<div>EventID : 52</div> <div>Event Time : Feb, 07, 2021, 04:24 AM</div> <div>Rule : SOC120 - Phishing Mail Detected - Internal to Internal</div> <div>Level : Security Analyst</div> <div>SMTP Address : 172.16.20.3</div> <div>Source Address : john@letsdefend.io</div> <div>Destination Address : susie@letsdefend.io</div> <div>E-mail Subject : Meeting</div> <div>Device Action : Allowed</div>					

Click on >> and create case and click Continue.

Incident Details	
Incident Name:	EventID: 52 - [SOC120 - Phishing Mail Detected - Internal to Internal]
Description:	EventID: 52
Incident Type:	Exchange
Created Date:	Jan, 11, 2024, 09:57 AM
<div>Start Playbook!</div>	

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.

Meeting	Q	OR	Detailed Search	▼
Date	Sender	Recipients	Subject	Final Action
Feb, 07, 2021, 04:24 AM	john@letsdefend.io	susie@letsdefend.io	Meeting	Unknown

<

From: john@letsdefend.io

To: susie@letsdefend.io

Subject: Meeting

Date: Feb, 07, 2021, 04:24 AM

Action: [Action](#)

🗑

Hi Susie, Can we arrange a meeting today if you are available?

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!

×

Parse Email

Before starting the analysis, information about the incoming email should be obtained.

- When was it sent?
- What is the email's SMTP address?
- What is the sender address?
- What is the recipient address?
- Is the mail content suspicious?
- Are there any attachment?

Next

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

×

Are there attachments or URLs in the email?

Please click "Yes" if there are an attachments or URLs in the email, if there are no attachments or URLs in the email please click "No".

Contains Attachment or Url?

NoYes

Selecting NO here.

×

Add Artifacts

+

Value	Comment	Type	Remove
172.16.20.3	SMTP address	IP Address ▾	

Next

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

×

Analyst Note

Please enter your analysis comments.

We see that there is no attachment or links which rules out that there could be a malicious intent. The email is personalized 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.
Not a phishing mail.

309 / 3000

Next

Not a Phishing Mail.

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

×

Close Alert

Event ID :

52

☒ True Positive ☐ False Positive


Note:

Internal mail between two colleagues with no links or attachments. Not a phishing mail.

Close 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.

SEVERITY	DATE CLOSED	RULE NAME	EVENTID	TYPE	RESULT	ACTION
Medium	Jan, 11, 2024, 10:19 AM	SOC120 - Phishing Mail Detected - Internal to Internal	52	Exchange	✓	
<div><div>EventID :</div><div>Event Time :</div><div>Rule :</div><div>Answer :</div><div>Playbook Answers :</div><div>Analyst Note :</div><div>Community Walkthrough :</div></div> <div><div>52</div><div>Feb, 07, 2021, 04:24 AM</div><div>SOC120 - Phishing Mail Detected - Internal to Internal</div><div>False Positive (+5 Point)</div><div>Are there attachments or URLs in the email? (+5 Point)</div><div>Internal mail between two colleagues with no links or attachments. Not a phishing mail.</div><div>Show</div></div>						

Hope this helped.