Introduction

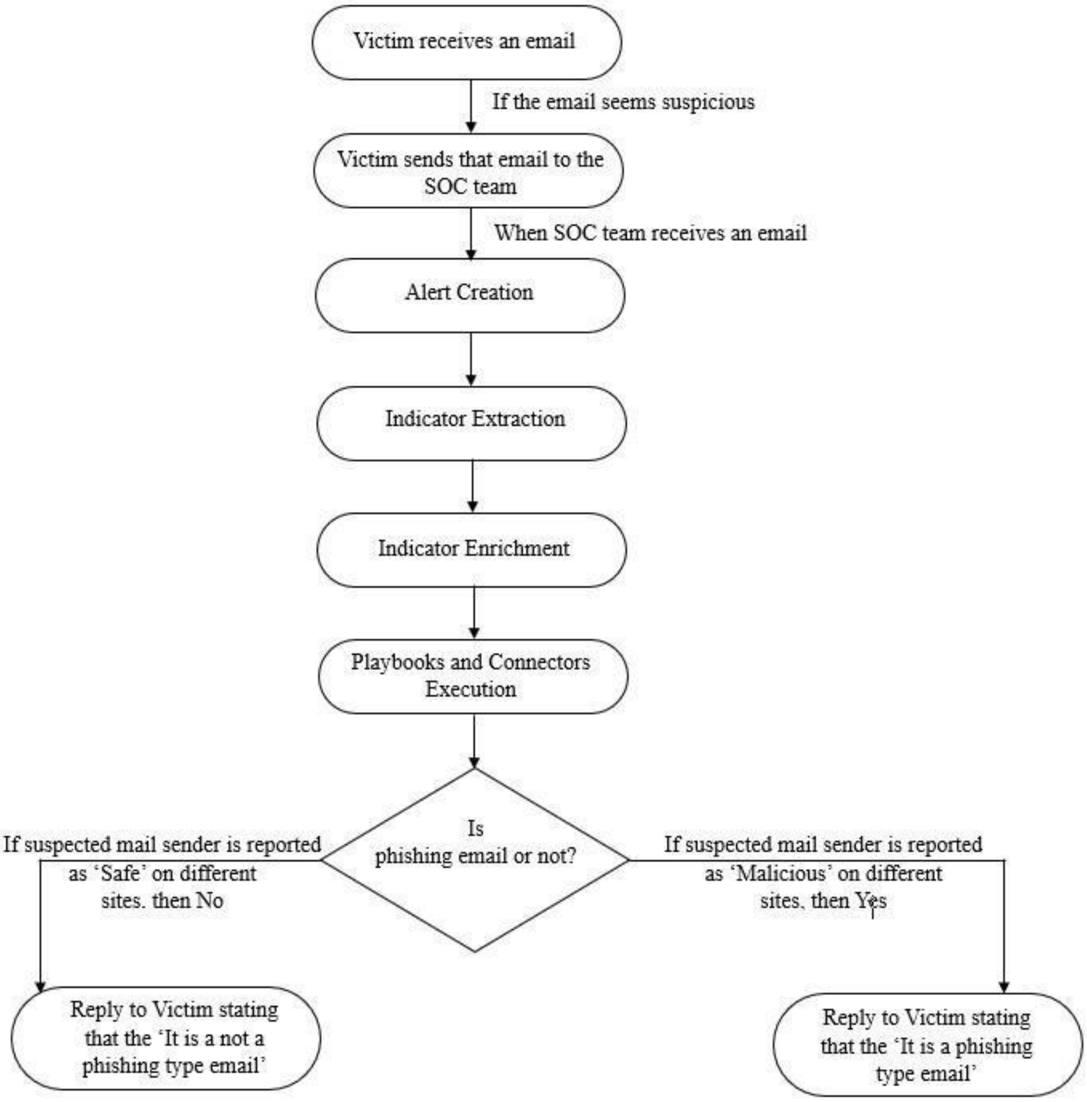
General

Email phishing scams are now a common and constantly evolving threat in the digital world. Email phishing is one of the most common methods of attack because attackers continuously develop new strategies to trick people and businesses. In an email phishing scam, attackers use false emails to fool people or organizations into providing sensitive information, such as login passwords, financial information, or personal information. Email phishing scams are a common and persistent type of cybercrime. These frauds frequently involve malicious motives, such as money theft, identity theft, or unlawful access to computer networks or systems.

This project is based on email phishing investigation. Using this project, one can save itself from being a victim of email phishing scam, be it an individual or an organization. The project tells us about the SOC team and gives a brief overview of phishing, especially through email. SOC stands for Security Operations Center. A SOC team is a group of cyber security members responsible for safeguarding an organization's digital assets, information, and technology infrastructure from security threats and incidents. Learning about email phishing is also provided in the project, which includes how phishing works, steps to respond to phishing, and malware. Malware is a type of software created by attackers to do harmful things without your permission. They steal information, spy on you, mess things up, etc. The most common malware used in phishing are ransomware, spyware, and adware.

This is an automated project. In this project, several playbooks and connectors are automated to investigate the phishing scam. The project uses FortiSOAR software, which has several playbooks on phishing. After automating those playbooks and configuring various connectors, this project can help investigate email phishing fraud. If anyone suspects an email to be fraudulent, they need to download that email and send it to the SOC team. As soon as the SOC team receives an email, an alert is automatically created, and steps such as indicator extraction and indicator enrichment start. After that, execution of various playbooks and connectors starts on that alert. If that sender is reported as suspicious, then that sender is marked as a phisher. If not, then the sender is given a clean chit. The sender of the suspected email is then replied with the message according to the status of the suspected mail sender.

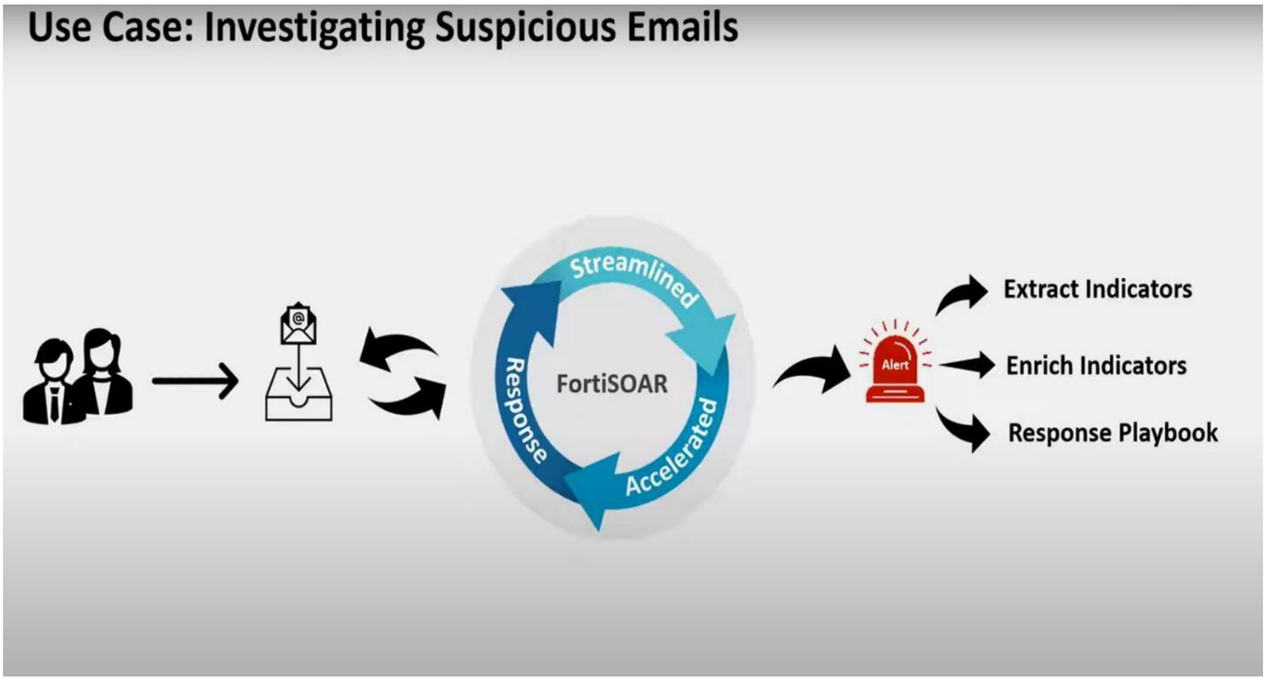
Working Flowchart


Victim receives an email
If the email seems suspicious
Victim sends that email to the SOC team
When SOC team receives an email
Alert Creation
Indicator Extraction
Indicator Enrichment
Playbooks and Connectors Execution
Is phishing email or not?
If suspected mail sender is reported as 'Safe' on different sites. then No
If suspected mail sender is reported as 'Malicious' on different sites. then Yes
Reply to Victim stating that the 'It is a not a phishing type email'
Reply to Victim stating that the 'It is a phishing type email'

Project Development

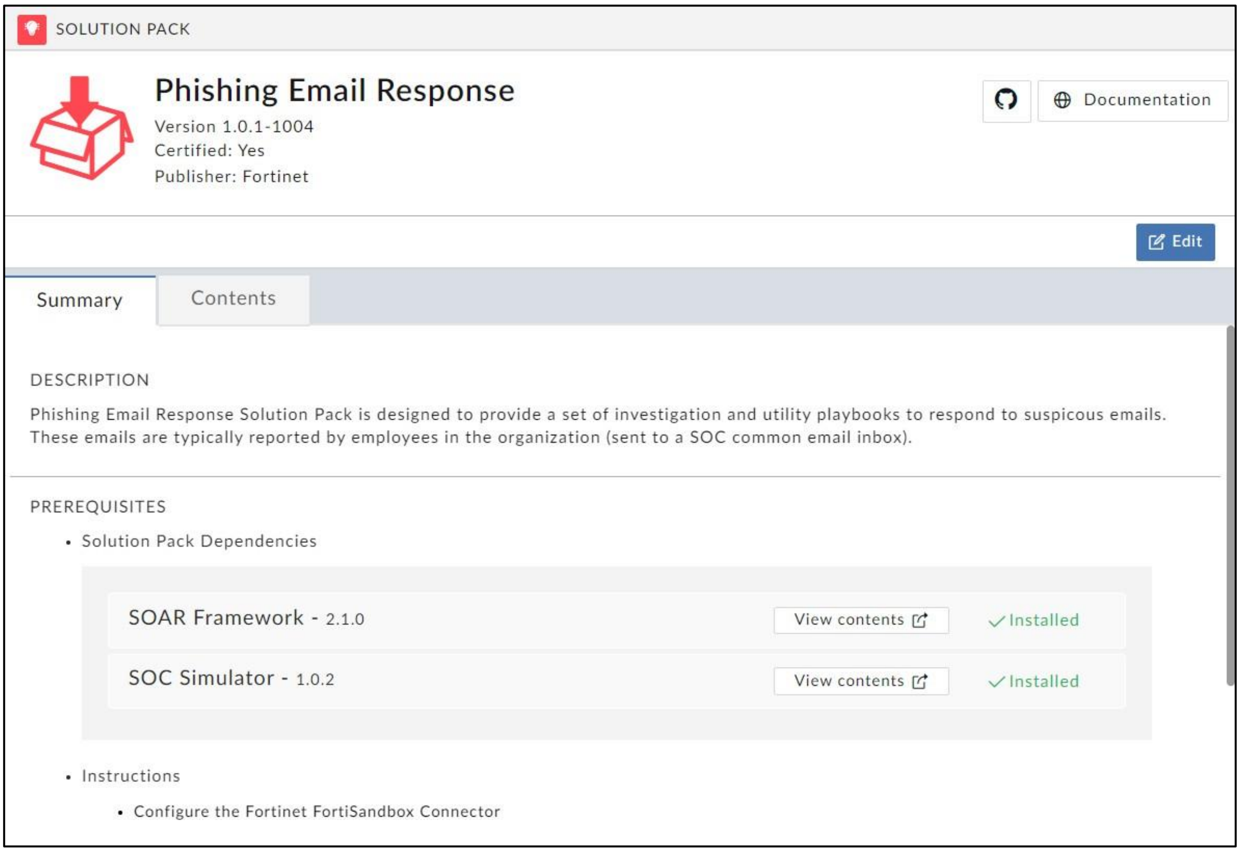
Scenario

I've automated the playbooks in this scenario so that we can investigate a suspicious email and determine whether or not it's a phishing email using the FortiSOAR software. As soon as the SOC team receives an email about a suspicious email, the automation process begins. An alert is automatically created with all the information required. Various fields of interest are extracted, and indicators are created. Various fields of interest are reporter information, email headers, senders, URLs, images, etc. The severity of the alert is judged on the basis of how malicious the indicators are. Then the playbook execution takes place. During the execution, an acknowledgement email is sent to the reporter. The execution starts with the SPF check, i.e., the Sender Policy Framework. SPF verifies that the reporter is authorized to send email for a specific domain or not. After this, spoofing is validated. Moving forward, suspicious keywords are flagged and malicious indicators are blocked (after confirmation). At last, a response email is sent to the reporter about the analysis of the reported email. The alert is closed, and the investigation is completed.


Use Case: Investigating Suspicious Emails

Solution Pack

The Phishing Email Response solution pack contains a set of investigation playbooks that help you respond to suspicious emails.



Phishing Email Response

Version 1.0.1-1004

Certified: Yes

Publisher: Fortinet

DESCRIPTION

Phishing Email Response Solution Pack is designed to provide a set of investigation and utility playbooks to respond to suspicous emails. These emails are typically reported by employees in the organization (sent to a SOC common email inbox).

PREREQUISITES

- Solution Pack Dependencies

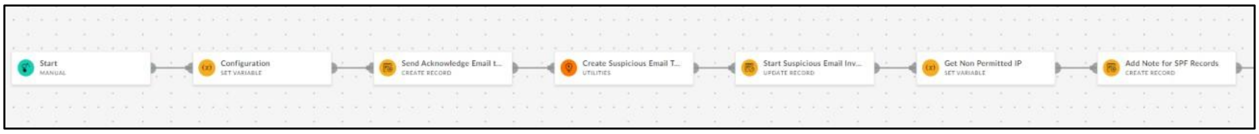
SOAR Framework - 2.1.0	View contents	✓Installed
SOC Simulator - 1.0.2	View contents	✓Installed

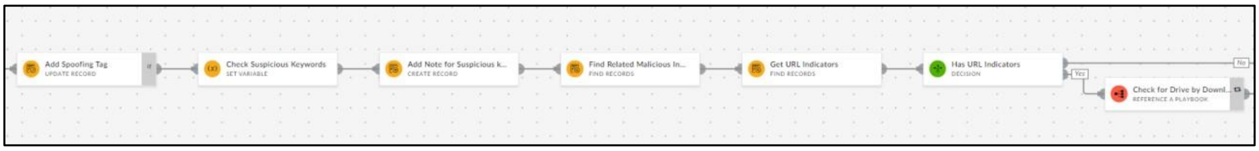
- Instructions
  - Configure the Fortinet FortiSandbox Connector

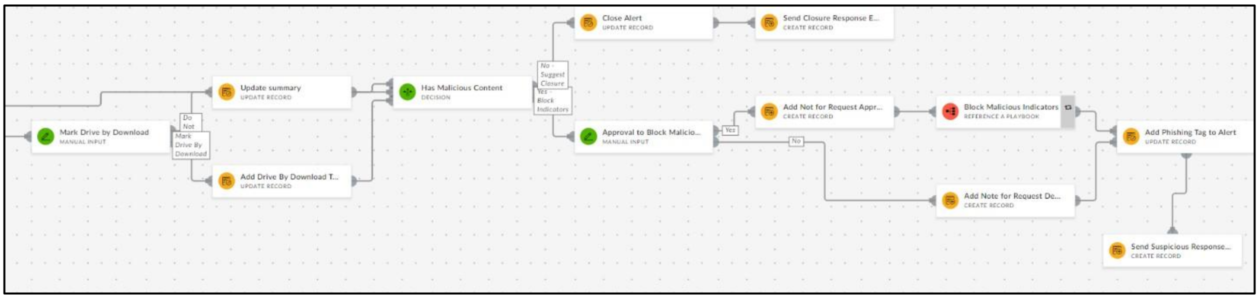
Playbooks Executed

Playbook 1: Investigate Suspicious Email

This playbook investigates an alert that is of the "Suspicious Email" type.



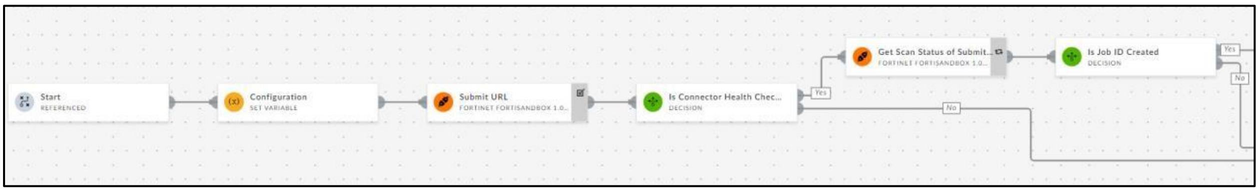


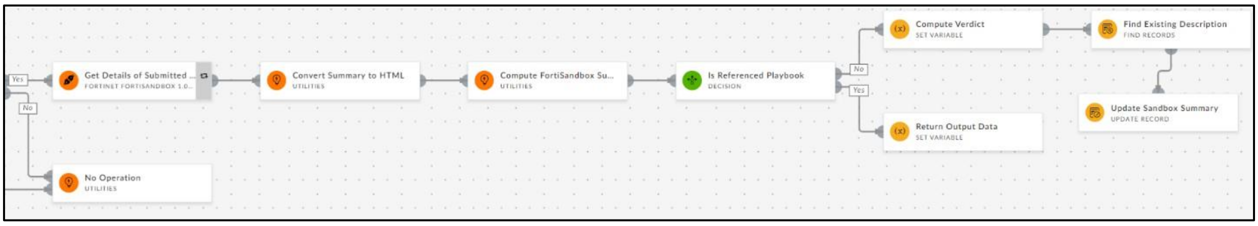


Playbook 2: URL > FortiSandbox > Enrichment

This playbook retrieves the reputation of an indicator of type URL using Fortinet Sandbox.

This is a Child Playbook that is referenced from the ‘Investigate Suspicious Email’ playbook.


Start
REFERENCED
Configuration
SET VARIABLE
Submit URL
FORTINET FORTISANDBOX 1.0...
Is Connector Health Chec...
DECISION
Yes
No
Get Scan Status of Submit...
FORTINET FORTISANDBOX 1.0...
Is Job ID Created
DECISION
Yes
No

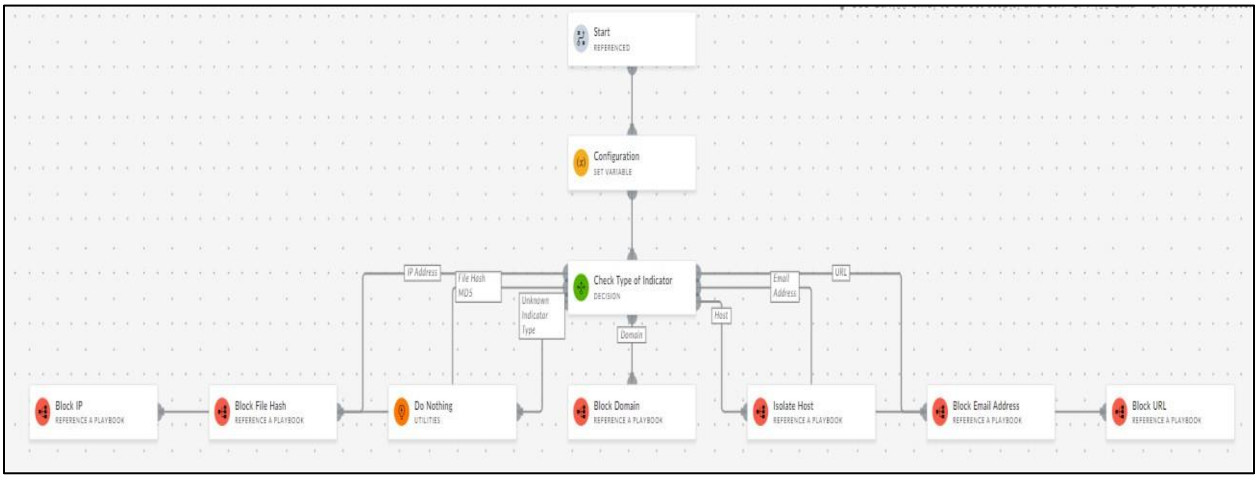


Playbook 3: Action (Type All) - Block Indicators

This playbook blocks all types of indicators on the firewall based on their block status.

This is a Child Playbook that is referenced from the ‘Investigate Suspicious Email’ playbook.

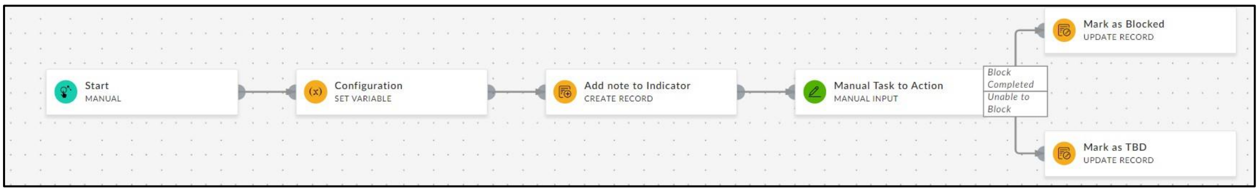
This playbook further refers to other playbooks that block indicators depending on various types.



Playbook 4: Action - IP Address - Block (Indicator)

This playbook blocks indicators of type 'IP Address' on the firewall and marks the indicators as "Blocked" based on their block status.

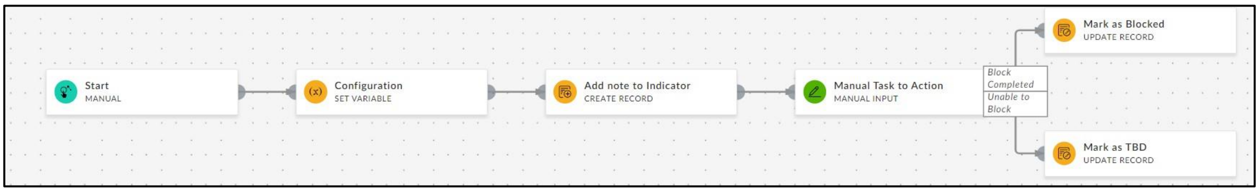
This is a Child Playbook that is referenced from the ‘Action (Type All) - Block Indicators’ playbook.



Playbook 5: Action - FileHash-MD5 - Block (Indicator)

This playbook blocks the indicators of type 'FileHash-MD5' on the firewall and marks the indicator as "Blocked" based on its block status.

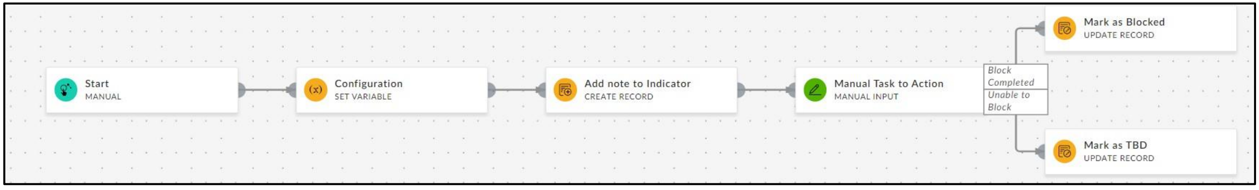
This is a Child Playbook that is referenced from the ‘Action (Type All) - Block Indicators’ playbook.



Playbook 6: Action - Action - Domain - Block (Indicator)

This playbook blocks the indicators of type 'Domain' on the firewall and marks the indicator as "Blocked" based on its block status.

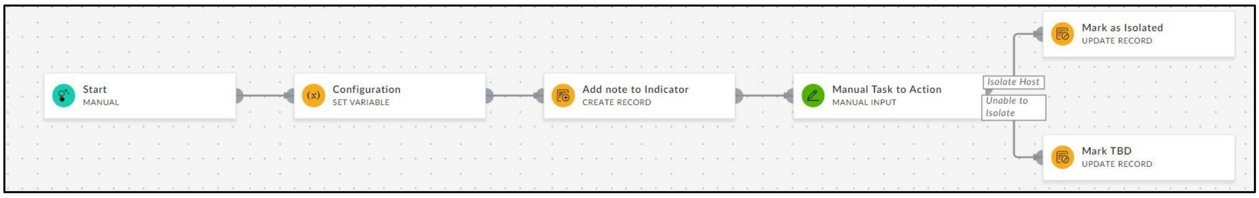
This is a Child Playbook that is referenced from the ‘Action (Type All) - Block Indicators’ playbook.



Playbook 7: Action - Action - Domain - Block (Indicator)

This playbook isolates indicators of type 'Host' and marks the indicator as "Isolated" based on its block status.

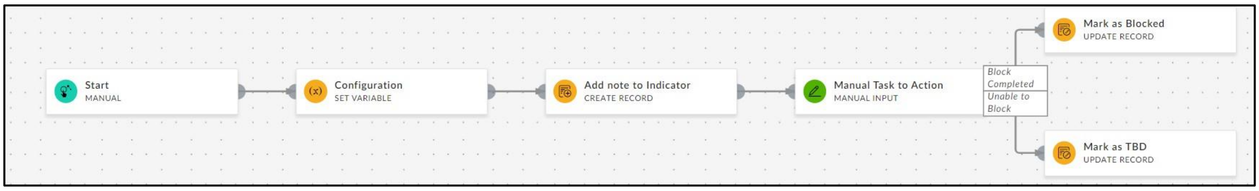
This is a Child Playbook that is referenced from the ‘Action (Type All) - Block Indicators’ playbook.



Playbook 8: Action - Email Address - Block (Indicator)

This playbook blocks the indicators of type 'Email Address' on the firewall and marks the indicator as "Blocked" based on its block status.

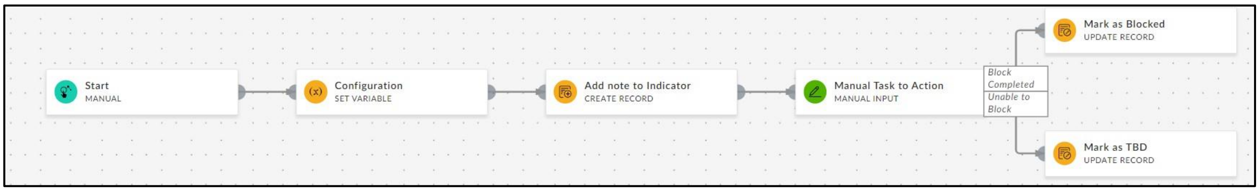
This is a Child Playbook that is referenced from the ‘Action (Type All) - Block Indicators’ playbook.



Playbook 9: Action - URL - Block (Indicator)

This playbook blocks the indicators of type 'URL' on the firewall and marks the indicator as "Blocked" based on its block status.

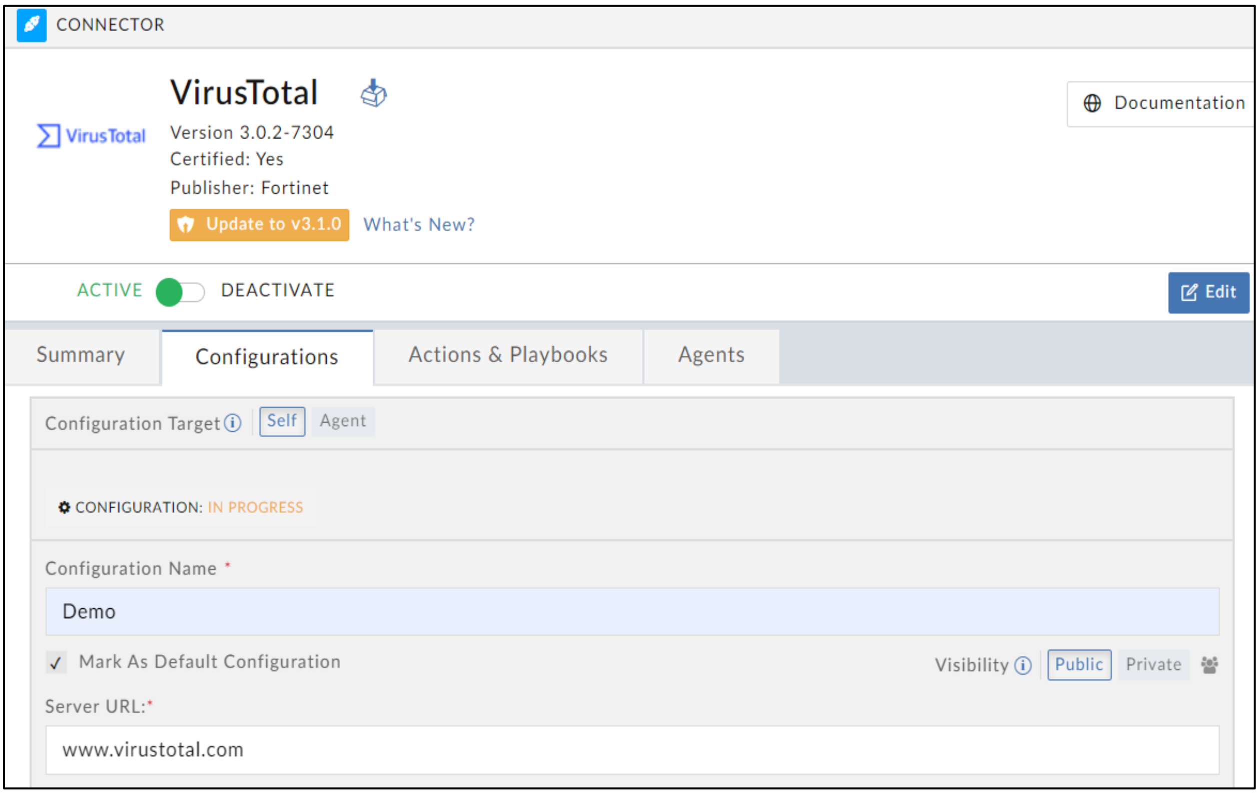
This is a Child Playbook that is referenced from the ‘Action (Type All) - Block Indicators’ playbook.



Connectors Used In The Scenario

VirusTotal

This is the VirusTotal Connector. It analyses suspicious files, domains, IPs, and URLs to detect malware and other breaches and automatically shares them with the security community.



VirusTotal

Version 3.0.2-7304

Certified: Yes

Publisher: Fortinet

Configuration Target: [✓ Self] Agent

CONFIGURATION: IN PROGRESS

Configuration Name *: Demo

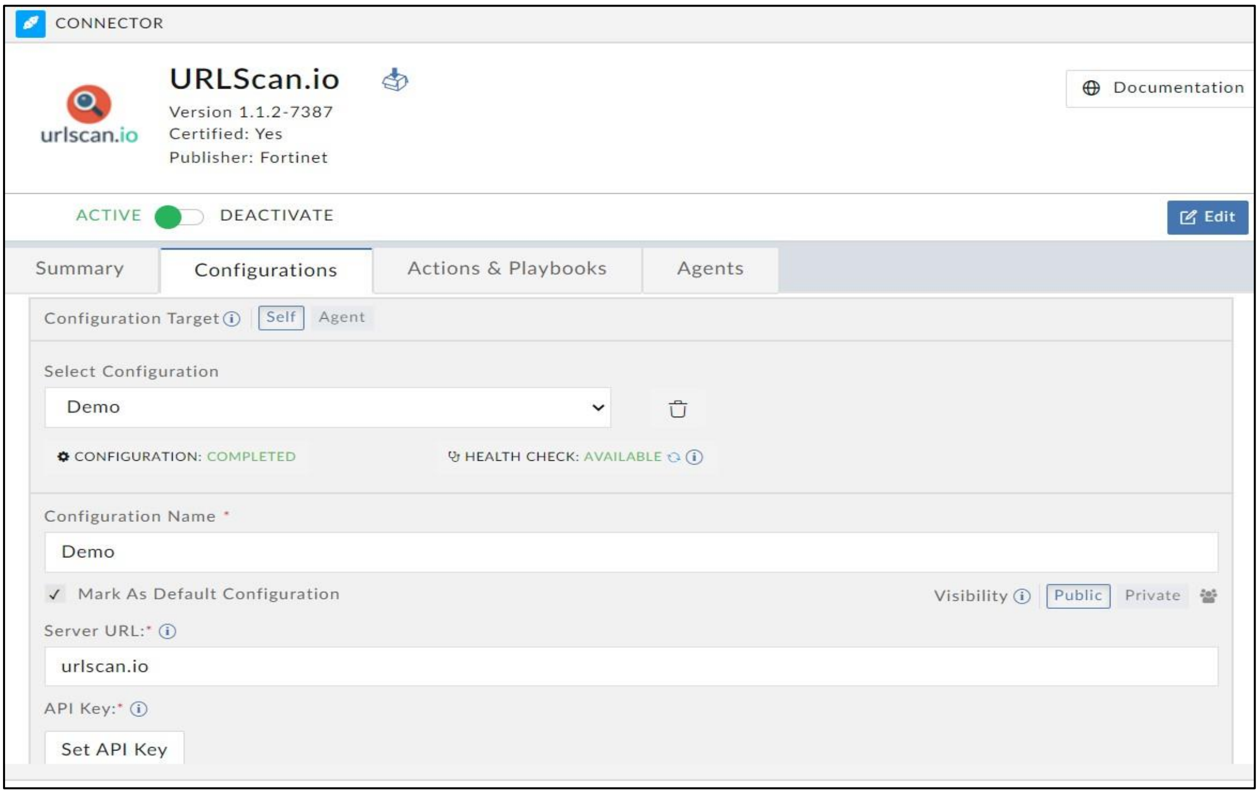
✓ Mark As Default Configuration

Visibility: [✓ Public] Private

Server URL:*: www.virustotal.com

URLScan.io

This is the URLScan.io connector. It provided tools for analysing and scanning websites and URLs for security issues. It captures screenshots, traces HTTP requests, checks for malicious activity, and provides detailed reports about potential threats.



CONNECTOR

URLScan.io

Version 1.1.2-7387

Certified: Yes

Publisher: Fortinet

ACTIVE DEACTIVATE

Configuration Target: Self

Select Configuration: Demo

CONFIGURATION: COMPLETED

HEALTH CHECK: AVAILABLE

Configuration Name *: Demo

✓ Mark As Default Configuration

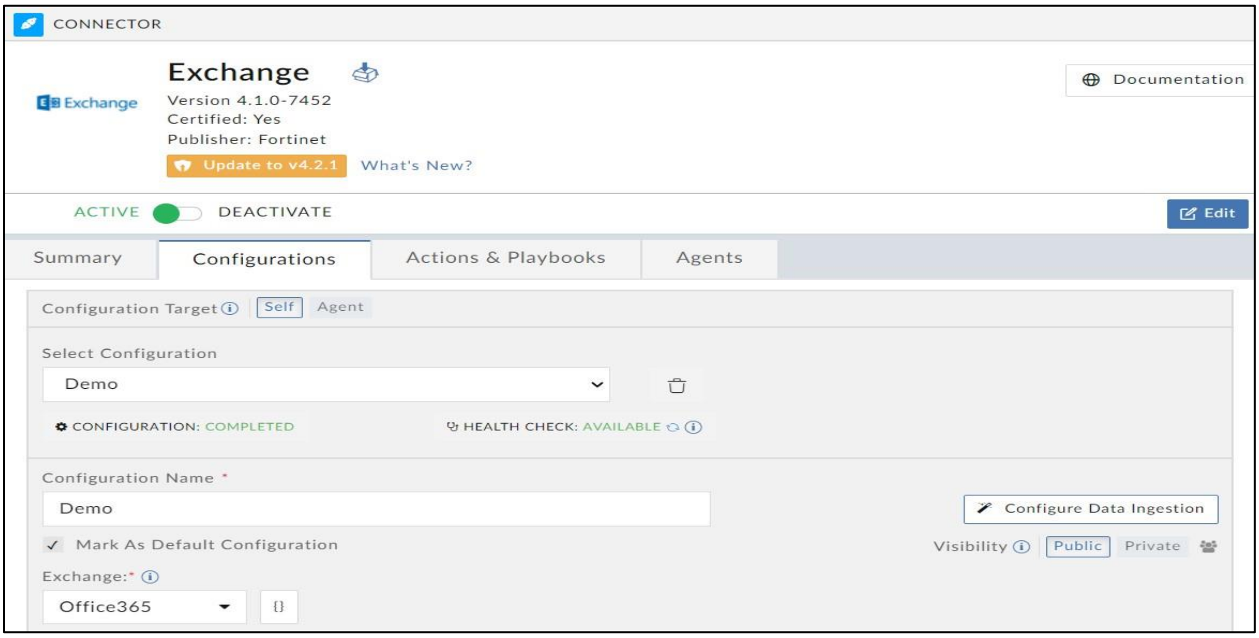
Visibility: Public

Server URL:*: urlscan.io

API Key:*: Set API Key

Exchange

This is the Exchange connector. It provides a reliable, platform-independent, and simple interface for communicating with Microsoft Exchange 2007-2016 Server or Office 365 using Exchange Web Services (EWS).



Exchange
Version 4.1.0-7452
Certified: Yes
Publisher: Fortinet

Configuration Target: Self | Agent

Select Configuration: Demo

CONFIGURATION: COMPLETED

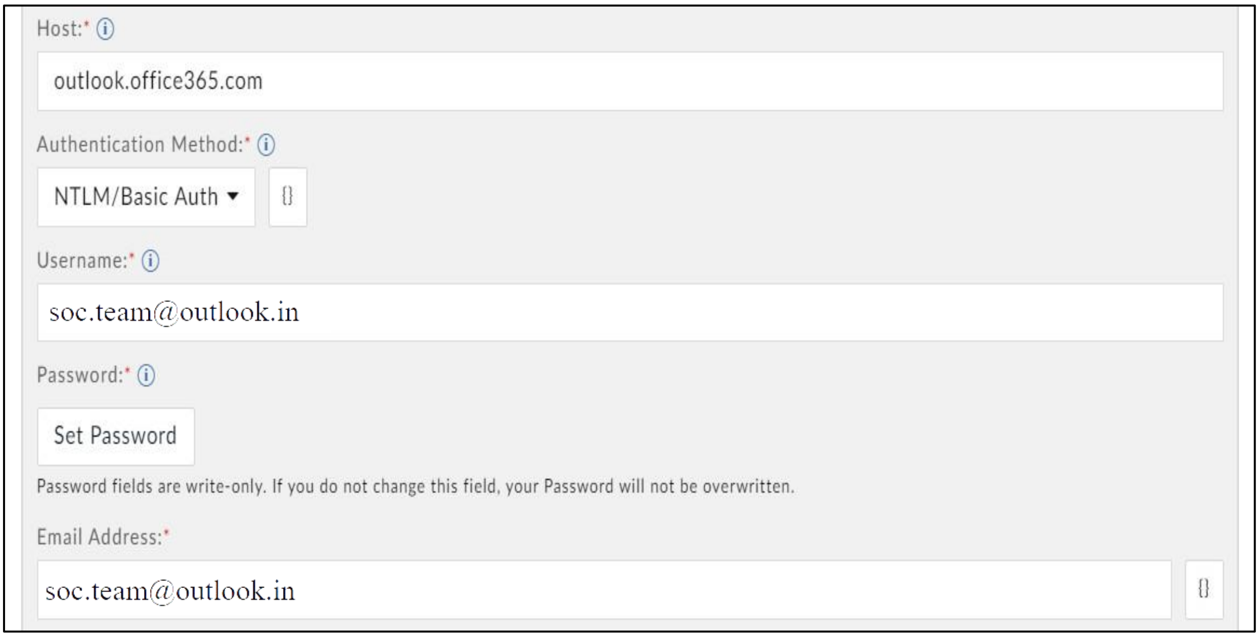
HEALTH CHECK: AVAILABLE

Configuration Name *: Demo

✓ Mark As Default Configuration

Visibility: Public | Private

Exchange:*: Office365



Host:*: outlook.office365.com

Authentication Method:*: NTLM/Basic Auth

Username:*: soc.team@outlook.in

Password:*: Set Password

Password fields are write-only. If you do not change this field, your Password will not be overwritten.

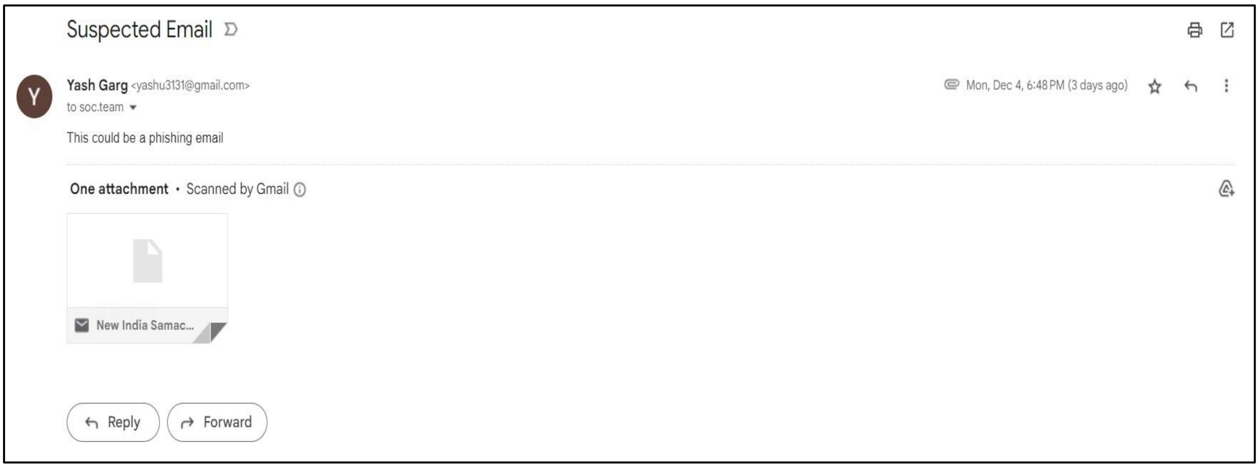
Email Address:*: soc.team@outlook.in

Reporter

A person who receives a suspicious email and wants to report it to the SOC team is referred to as a reporter.

Yash Garg is the reporter in both the cases and is sent an email that appears suspicious and might be a phishing email. In order to investigate, he emails the SOC team to inform them that a suspicious email has been received. Also included is the received suspicious email.

Case 1:



Suspected Email

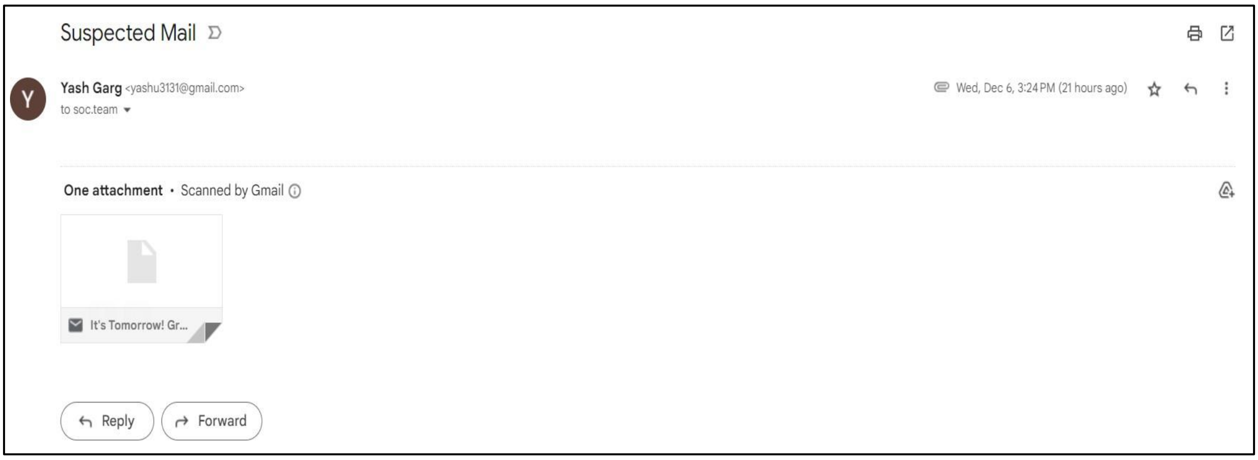
Yash Garg <yashu3131@gmail.com>
to soc.team

Mon, Dec 4, 6:48 PM (3 days ago)

This could be a phishing email

One attachment • Scanned by Gmail

Case 2:



Suspected Mail

Yash Garg <yashu3131@gmail.com>
to soc.team

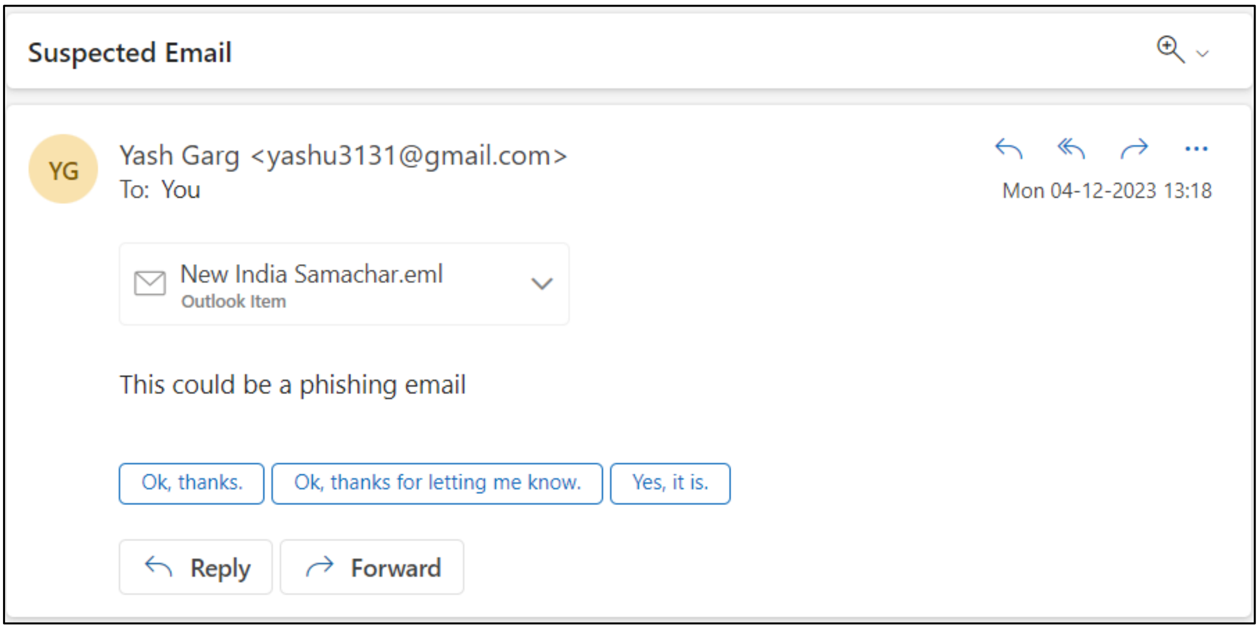
Wed, Dec 6, 3:24 PM (21 hours ago)

One attachment • Scanned by Gmail

SOC Inbox

When the SOC team receives a reported email about phishing, the process begins.

Case 1:



Suspected Email

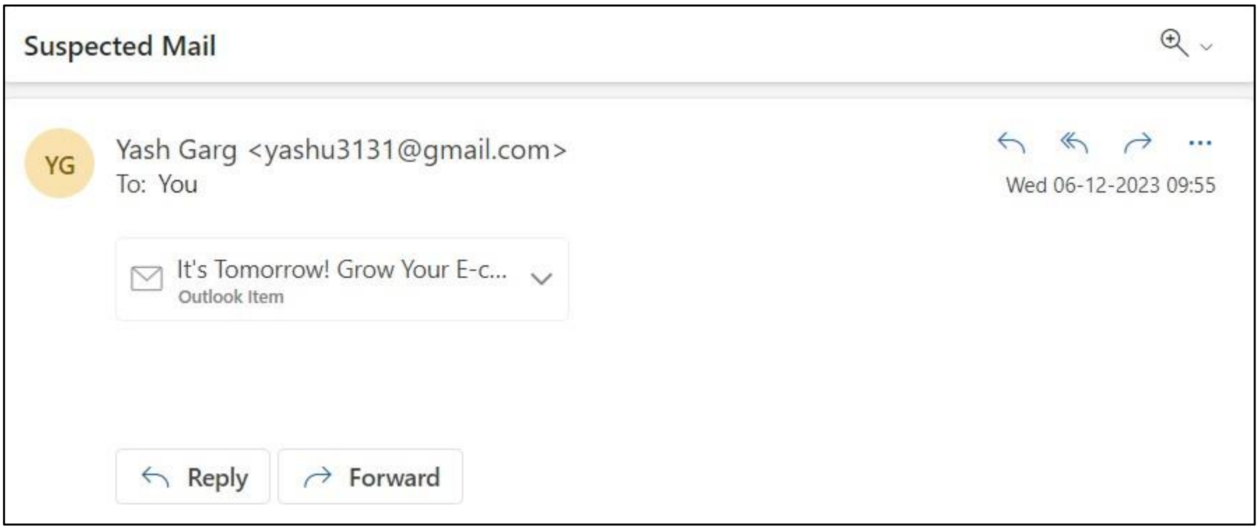
Yash Garg <yashu3131@gmail.com>
To: You

Mon 04-12-2023 13:18

New India Samachar.eml
Outlook Item

This could be a phishing email

Case 2:



Suspected Mail

Yash Garg <yashu3131@gmail.com>
To: You

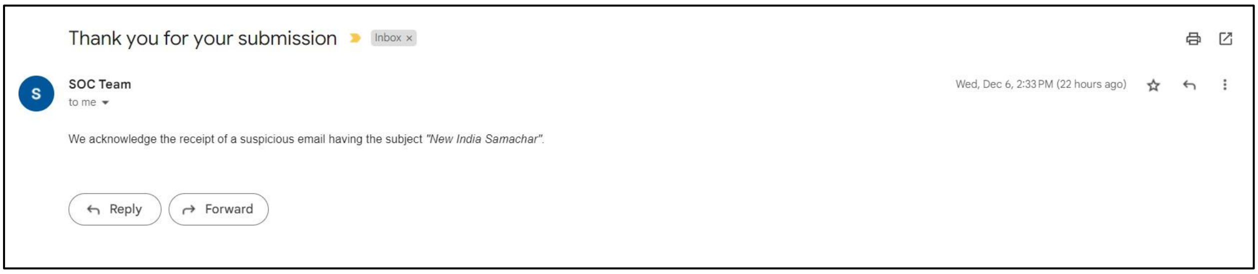
Wed 06-12-2023 09:55

It's Tomorrow! Grow Your E-c...
Outlook Item

Acknowledgement from SOC Team

When SOC team receives an email, it sends an acknowledgement email to the reporter about their reported email.

Case 1:



Thank you for your submission

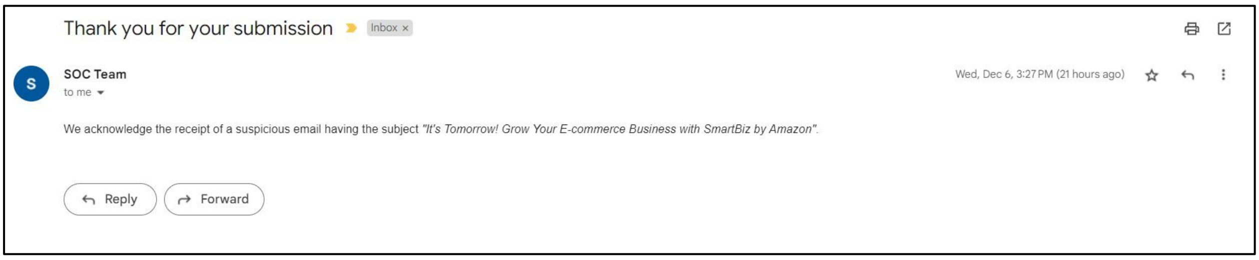
SOC Team

to me

Wed, Dec 6, 2:33 PM (22 hours ago)

We acknowledge the receipt of a suspicious email having the subject *"New India Samachar"*.

Case 2:



Thank you for your submission

SOC Team

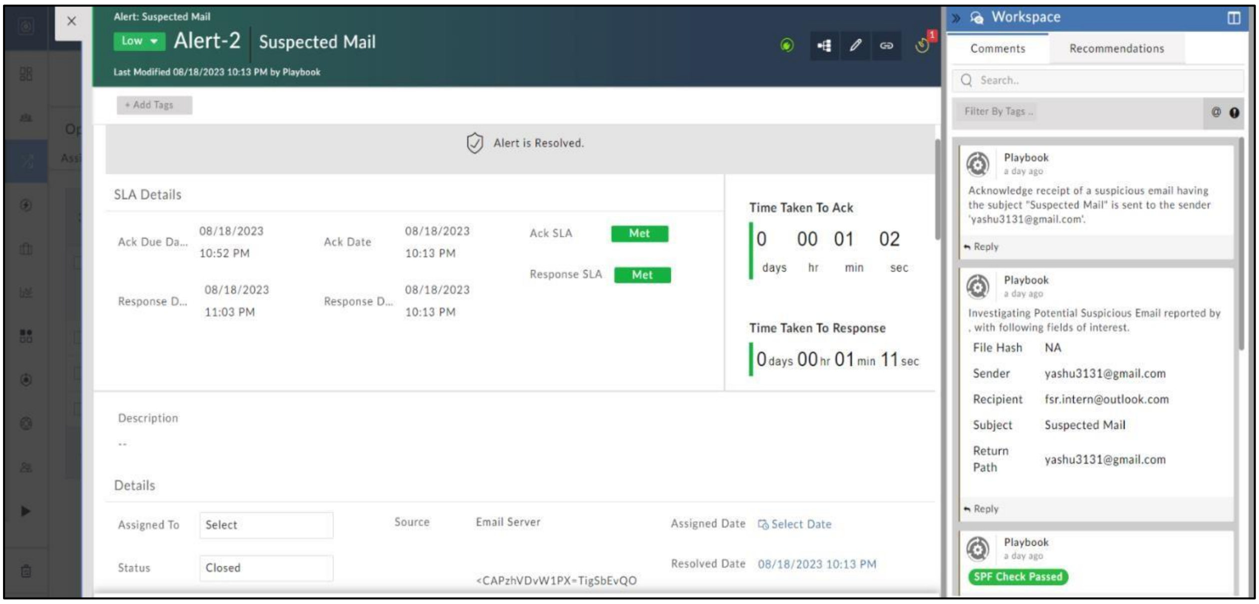
to me

Wed, Dec 6, 3:27 PM (21 hours ago)

We acknowledge the receipt of a suspicious email having the subject *"It's Tomorrow! Grow Your E-commerce Business with SmartBiz by Amazon"*.

Investigation Process

An alert is automatically generated as soon as an email enters the SOC Inbox, the case-specific playbooks are carried out, and the investigation starts. Firstly, all the images, URLs, keywords etc are extracted and diagnosed using different connectors that are configured during the automation. Email is them tested in a Sandbox. After all the investigation, the email is reported as phishing type or not.



Last Modified 08/18/2023 10:13 PM by Playbook

Alert is Resolved.

SLA Details

Ack Due Da...	08/18/2023 10:52 PM	Ack Date	08/18/2023 10:13 PM	Ack SLA	Met
Response D...	08/18/2023 11:03 PM	Response D...	08/18/2023 10:13 PM	Response SLA	Met

Time Taken To Ack

0 days 00 hr 01 min 02 sec

Time Taken To Response

0 days 00 hr 01 min 11 sec

Description

--

Details

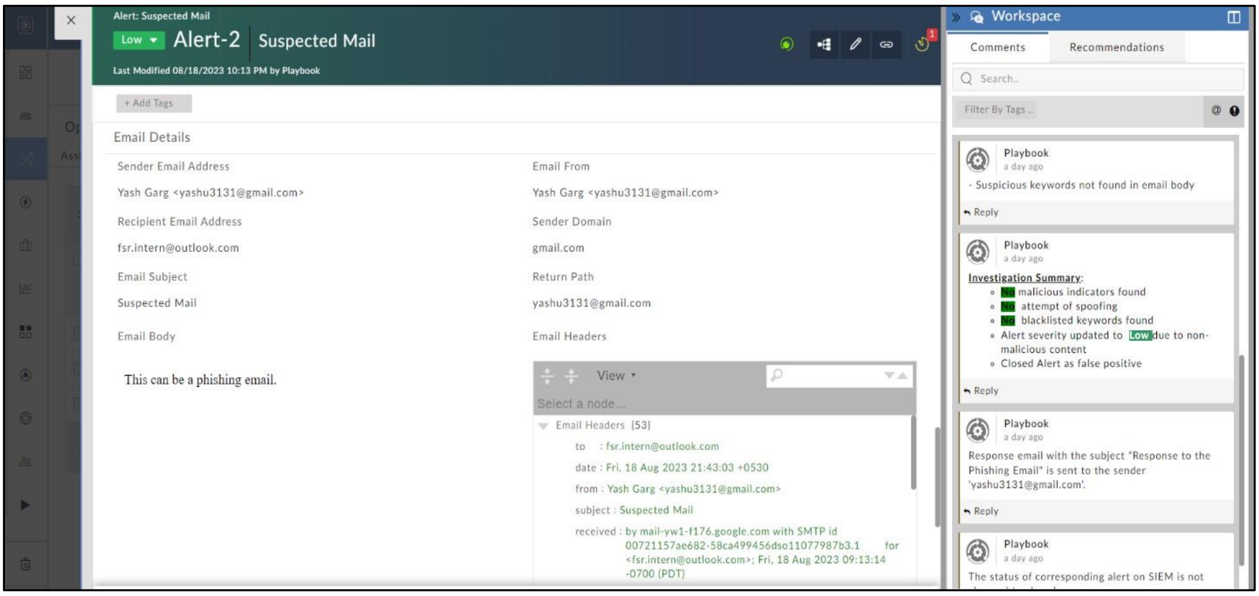
Assigned To: Select
Source: Email Server
Assigned Date: Select Date
Status: Closed
Resolved Date: 08/18/2023 10:13 PM
<CAPzhVDvW1PX=TigSbEvQO

Playbook
a day ago
Acknowledge receipt of a suspicious email having the subject "Suspected Mail" is sent to the sender 'yashu3131@gmail.com'.

Playbook
a day ago
Investigating Potential Suspicious Email reported by , with following fields of interest.

File Hash	NA
Sender	yashu3131@gmail.com
Recipient	fsr.intern@outlook.com
Subject	Suspected Mail
Return Path	yashu3131@gmail.com

Playbook
a day ago
SPF Check Passed



Last Modified 08/18/2023 10:13 PM by Playbook

Email Details

Sender Email Address
Yash Garg <yashu3131@gmail.com>

Email From
Yash Garg <yashu3131@gmail.com>

Recipient Email Address
fsr.intern@outlook.com

Sender Domain
gmail.com

Email Subject
Suspected Mail

Return Path
yashu3131@gmail.com

Email Body

This can be a phishing email.

Email Headers

```
Email Headers {53}
    to    : fsr.intern@outlook.com
    date : Fri, 18 Aug 2023 21:43:03 +0530
    from : Yash Garg <yashu3131@gmail.com>
    subject : Suspected Mail
    received : by mail-yw1-f176.google.com with SMTP id
               00721157ae682-58ca499456dso11077987b3.1      for
               <fsr.intern@outlook.com>; Fri, 18 Aug 2023 09:13:14
               -0700 (PDT)
```

Playbook
a day ago
- Suspicious keywords not found in email body

Playbook
a day ago
Investigation Summary:
- No malicious indicators found
- No attempt of spoofing
- No blacklisted keywords found
- Alert severity updated to Low due to non-malicious content
- Closed Alert as false positive

Playbook
a day ago
Response email with the subject "Response to the Phishing Email" is sent to the sender 'yashu3131@gmail.com'.

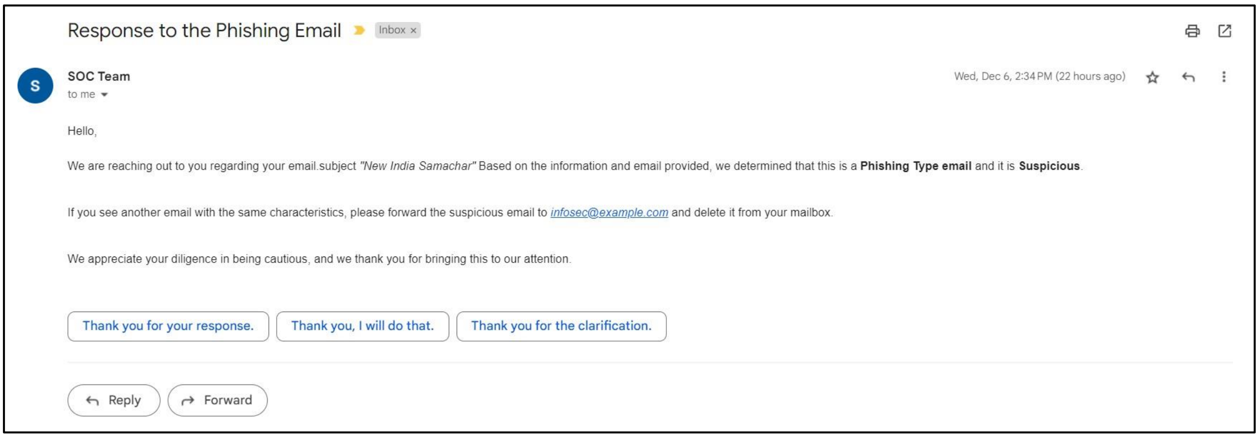
Playbook
a day ago
The status of corresponding alert on SIEM is not

Result Analysis

Response

Through an email reply, the SOC team informs the reporter that the investigation is complete and lets them know if the email is phishing or not.

Case 1: When the reported email was of the phishing type.



Response to the Phishing Email

SOC Team
to me

Wed, Dec 6, 2:34 PM (22 hours ago)

Hello,

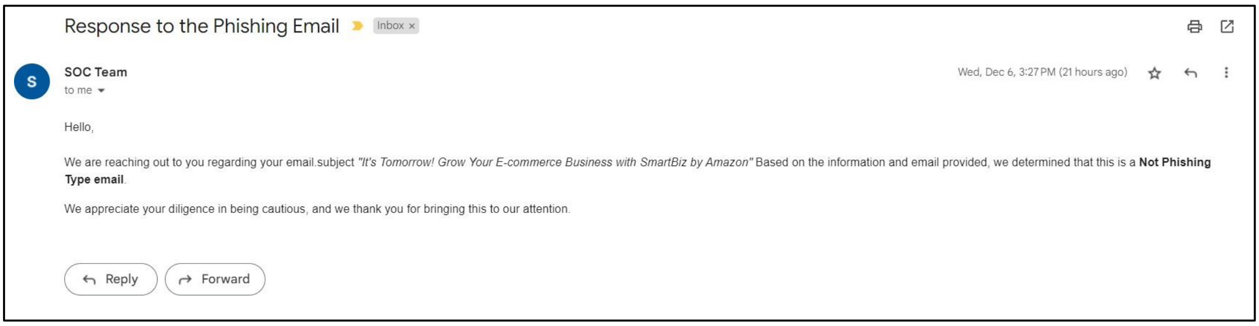
We are reaching out to you regarding your email.subject *"New India Samachar"* Based on the information and email provided, we determined that this is a **Phishing Type email** and it is **Suspicious**.

If you see another email with the same characteristics, please forward the suspicious email to *infosec@example.com* and delete it from your mailbox.

We appreciate your diligence in being cautious, and we thank you for bringing this to our attention.

Inbox ×
S
Thank you for your response.
Thank you, I will do that.
Thank you for the clarification.
Reply
Forward

Case 2: When the reported email was not of the phishing type.



Response to the Phishing Email

SOC Team
to me

Wed, Dec 6, 3:27 PM (21 hours ago)

Hello,

We are reaching out to you regarding your email.subject *"It's Tomorrow! Grow Your E-commerce Business with SmartBiz by Amazon"* Based on the information and email provided, we determined that this is a **Not Phishing Type email**.

We appreciate your diligence in being cautious, and we thank you for bringing this to our attention.