CYWARE™

Use Case

Spearphishing Response Automation

Staying Off the Hook

Spearphishing is one of the most common attack vectors for cybercriminals to infiltrate organizations globally. Phishing attack emails require relatively less effort on the part of attackers as they tend to exploit the human vulnerabilities that stand out as the weakest link in the security ecosystem. Thus, attackers can target an organization's employees, customers, or partners, through large-scale malspam campaigns or through specially-crafted spearphishing emails meant to deceive targeted individuals. Responding to spearphishing attacks on a continuous basis is a major challenge for security teams due to the sheer volume of such emails encountered on a daily basis.

Saving the Fish with Automation

To combat spearphishing threats in a rapid and effective manner, security teams can utilize automated spearphishing response playbooks. The automated playbooks standardize the response process from detection to blocking of the malicious indicators from where attacks are sourced.

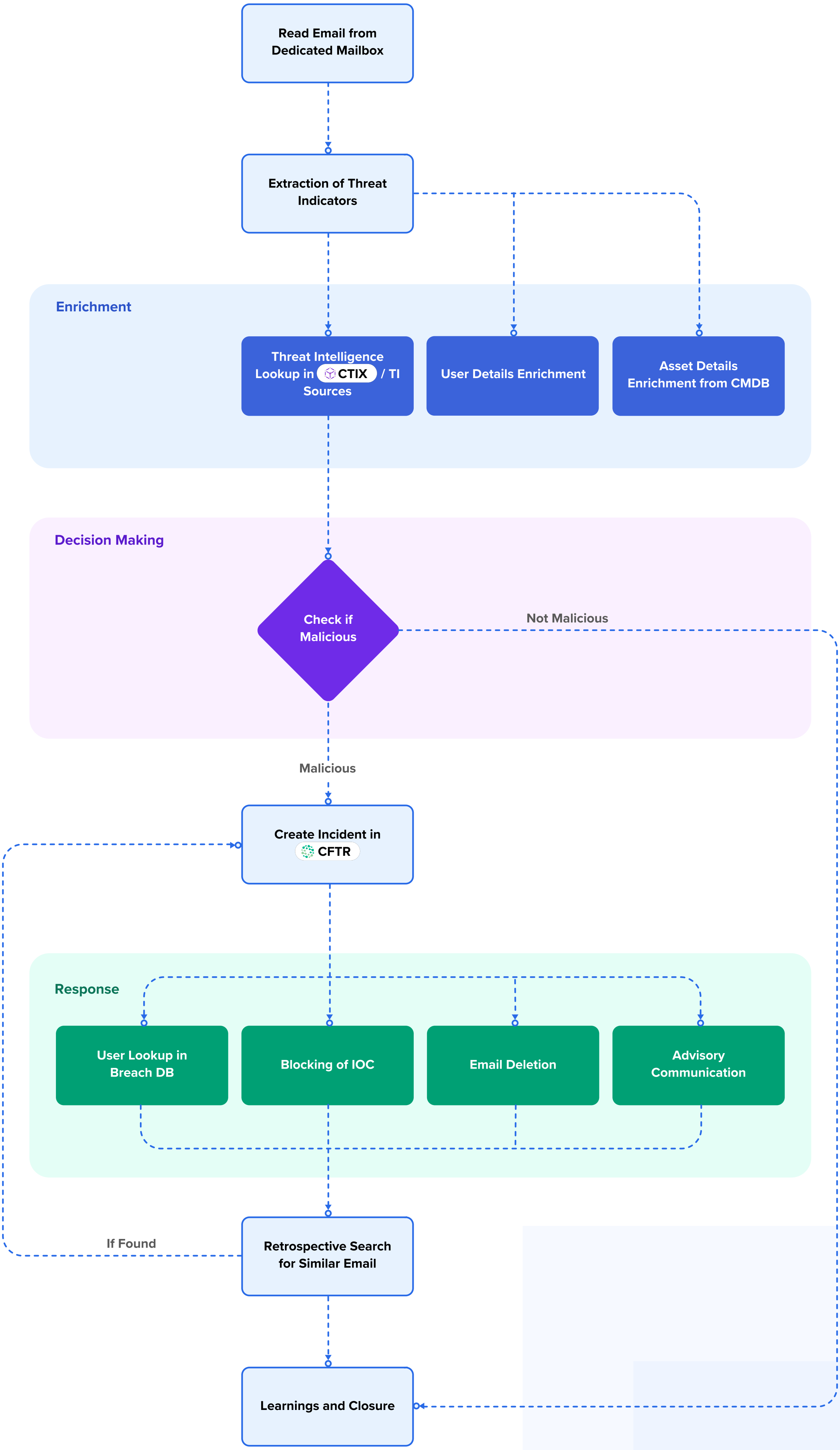
The spearphishing response playbook performs the following tasks

Poll Dedicated Mailbox

The playbook kickstarts the phishing handling response with the polling of the dedicated mailbox on the configurable interval over the IMAP/POP3 protocol to receive the phishing emails reported by the users

Identifying Threat Indicators

Once a phishing email is reported, It analyzes the suspicious email diligently for elements in the email headers, body, and attachments and automatically extracts relevant indicators of compromise (IOCs) such as embedded links, files, IPs, domains, email attachments, etc.


Read Email from Dedicated Mailbox
Extraction of Threat Indicators
Enrichment
Threat Intelligence Lookup in CTIX / TI Sources
User Details Enrichment
Asset Details Enrichment from CMDB
Decision Making
Check if Malicious
Not Malicious
Malicious
Create Incident in CFTR
Response
User Lookup in Breach DB
Blocking of IOC
Email Deletion
Advisory Communication
If Found
Retrospective Search for Similar Email
Learnings and Closure

Enrichment and Analysis

The collected IOCs are then enriched with information from several entities including CTIX and other TI sources and automated triaging is done by the conditional nodes of the playbook to rate the threat level of the reported email.

As in many cases, if the threat is found to be a false-positive then additional steps are performed:

- Run a check on Sandbox.
- Past history of the extracted indicators
- Inspect the sender's domain with the historical DNS information

Response Actions

Based on the triaging information, several response actions are initiated in real-time such as

- Blocking the sender's email address
- Blocking malicious IOCs
- Adding IOCs to the watchlist of SIEM solution
- Looking up the email recipient to the breach DB
- Email deletion from other mailbox and advisory notification to all the impacted users
- Keeping the threat quarantined for manual investigation

Defining the Threat Horizon

The playbook automatically performs the retrospective hunt across various security technologies to identify similar threat indicators across the organization. Thereafter, an automated alert is triggered to warn the affected users.

End-to-end response ensures that not only the current attack is responded to, but all possible future attacks in the similar lines of the kill chain are also prevented.

Cyware Advantage

Analyze Large Volumes of Phishing Emails

By leveraging security automation in the response process, security analysts can save time and effectively respond to a large volume of spearphishing alerts.

Track Targeted Attack Campaigns

Through automated IOC extraction and enrichment with data from multiple sources, analysts can understand and counter the tactics, techniques, and procedures used by specific threat actors.

Stop a variety of attacks at an early stage

The playbook helps analyze a spearphishing threat in the context of the entire attack lifecycle to help block threat actors that use it as a means to infiltrate networks and deploy malicious exploits.

Going Beyond Incident Investigation

The playbook not only just helps the organization to respond to specific phishing threats but also helps capture the long term learnings from the incidents to put in place the long term strategic controls to thwart any such future attempts by using the unique capabilities of the fusion center.

CYWARE™

111 Town Square Place Suite 1203,
#4 Jersey City, NJ 07310

cyware.com | sales@cyware.com

☎ 855-MY-CYWARE