DEMISTO
Phishing Playbook Summary

THE CHALLENGE

Phishing is the most all-pervasive cyberattack out there today. It is a potent vector for other attacks – 91% of cyberattacks in 2016 started with a phishing email[1] . It affects organizations across industries and functions, with 85% of organizations suffering phishing attacks in 2016[2] . It is also very simple for attackers to craft, resulting in an attack volume and velocity that SOCs and analysts can't keep up with. Analysts need a phishing response that is fast, handles large volumes, standardized to deal with repeated attacks, and still customizable to deal with unique attacks.

THE DEMISTO PHISHING PLAYBOOK

Demisto provides an out-of-the-box phishing response playbook that helps analysts contain phishing attacks at every step of the kill chain. Here are the main advantages of using the playbook:

SIMPLE AND INTUITIVE: The playbooks are represented as a task/process flow through a simple drag-and-drop graphical interface. No coding expertise is required to make even the most complex playbooks, although each playbook's code is also available for analysts to tweak if required.

PRIMED FOR AUTOMATION: Analysts can automate the entire playbook in response to a phishing attack, greatly reducing response time, effort, and the possibility of human error for large-volume attacks. However, analysts can also choose to include manual steps and require human intervention for sophisticated attacks.

CUSTOMIZABLE: Analysts can make copies of the standard playbook to modify it or embed it in other playbooks as needed.

HOW IT WORKS

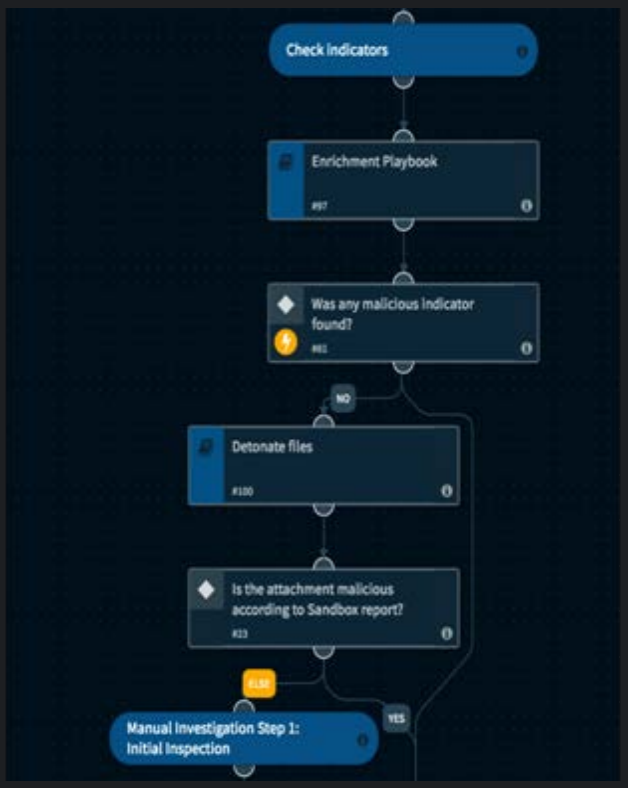
TRIAGE AND ENGAGE

- **WHY:** When an employee sends you a suspected phishing email, it's important to assume malice until proven otherwise. Apprising the employee of email receipt puts them at ease, and initial triage helps gauge the severity of the phishing attack in question.
- **STEPS:** Store the employee email account that sent the alert and send a mail to them confirming receipt. Enrich the account with details from Active Directory and add phishing email data to relevant context entities.

[1]Source: Dark Reading (http://www.darkreading.com/endpoint/91--of-cyberattacks-start-with-a-phishing-email/d/d-id/1327704)
[2]Source: Barkly (https://blog.barkly.com/phishing-statistics-2016)

EXTRACT INDICATORS

- **WHY:** Extracting common indicators helps break the phishing email down to constituent parts and kickstarts initial investigation.
- **STEPS:** Extract the IP address and URL from the phishing email.



CHECK INDICATORS

- **WHY:** Extracted indicators need added context, which analysts can provide by enriching them with reputation from integrated security tools. This is the first branch where indicator malice is checked.
- **STEPS:** Enrich data with reputation from sources like File, URL, and IP. Use conditional task to check if malicious indicator was found.

INVESTIGATING FALSE POSITIVES

- **WHY:** Checks for false positives should involve many steps and be comprehensive, because the alternative is still far more pernicious. Many of these steps can be automated, which keeps (and even increases) the level of robustness while reducing analyst effort and manual labor.
- **STEPS:** If no malicious indicators were found on initial check, run a check on Sandbox. If Sandbox results give the all clear, manually inspect the sender's domain distance to check closeness with the company's own domains. If there's nothing suspicious with the domain, check if the hostname URL is being misrepresented. If the mail passes all these tests, conduct one final manual investigation and pull in other security personnel if needed. It's now okay to send an email to the employee in question marking the email as safe, and the investigation can be closed.

RESPONDING TO VERIFIED PHISHING ATTEMPT

- **WHY:** If any of the false positive checks throw up a red flag, it's critical that analysts move to contain and respond to the threat immediately. Employees should be notified of confirmed malice, the attack's spread should be studied and curtailed, and the email's attachments should be investigated for further threats. This end-to-end response ensures that not only is the current attack responded to, but possible knock-on attacks in the kill chain are also prevented.
- **STEPS:** Send email to employee that the email is malicious and currently being responded to. Search other mailboxes for the phishing mail and delete all instances. If the email had an attachment and its hash was extracted, investigate it for malicious Indicators of Compromise using the tools at your disposal. If there was no attachment, close the investigation.

This summary demonstrates the comprehensive nature in which Demisto playbooks deal with phishing attacks. These playbooks are simple and intuitive to use, primed for automation, ideally involve interplay between machine-led and human-led tasks, and are customizable to fit analyst needs.