LogicHub

USE CASE

Phishing Triage

How to Automate and Accelerate Your Phishing Triage

The triage of reported phishing emails is time-consuming work and an analytical challenge for Security Operations Center (SOC) and Incident Response (IR) teams. It is critical that these security teams find a way to accelerate phishing triage, so they can spend less time investigating false positives phishing alerts and more time on valuable and strategic projects. LogicHub Phishing Triage is a solution for the triage of reported phishing emails. Powered by Machine Learning (ML), LogicHub Phishing Triage automatically and accurately analyzes and classifies emails on a customizable scale, such as *malicious*, *safe*, or *needs further review*. An intuitive interface lets security analysts quickly review results and kick off response workflows with a click.

In typical customer scenarios, LogicHub is able to achieve 97% accuracy and reduce the number of alerts requiring human analysis by 75% or more. Phishing Triage is available as an application, as a service, and as a customizable environment for building and editing your own flows and playbooks for advanced users or with the help of our services team.

Phishing Triage Challenges

- Hundreds of suspected phishing (and spam) emails are submitted daily to a single shared inbox
- Every email takes several minutes for an analyst to investigate
- Difficult for analysts to find and prioritize the most severe phishing alerts each day
- Manual playbooks make it impossible to investigate every alert, leading to analyst fatigue and inconsistencies in triage
- Difficult to retain learned threat intelligence and improve institutional knowledge

Solution

The LogicHub solution incorporates best practices in phishing email analysis and triage:

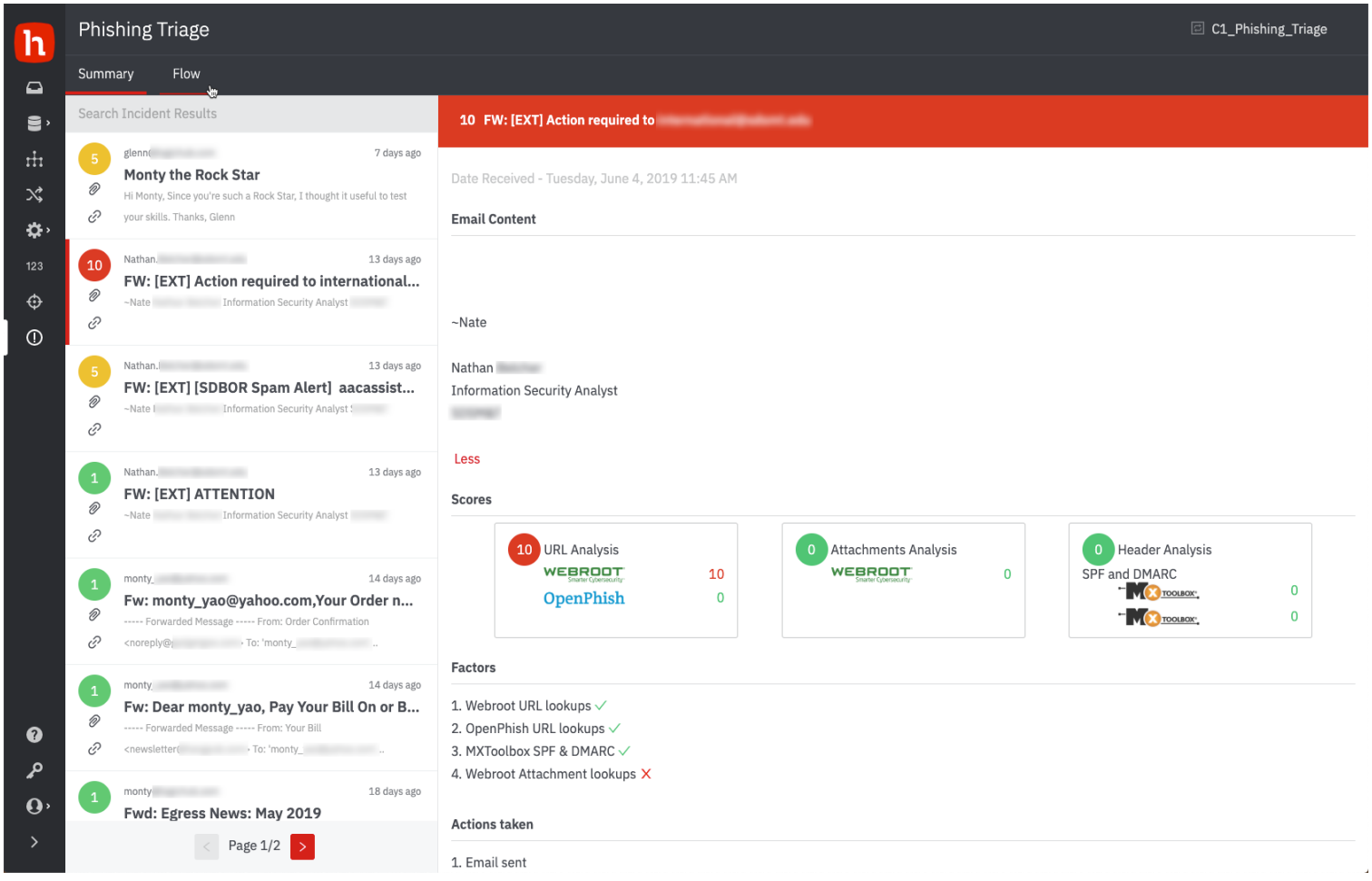
- Reads and parses email from a phishing mailbox (Exchange, IMAP, etc.).
  - Emails and attachments need to be brought into LogicHub for phishing analysis.
    - A designated mailbox is monitored for user-submitted suspected phishing emails which LogicHub accesses via the built-in email integration.
  - LogicHub runs each email through a dedicated purpose built EML file parser. This parser:
    - Breaks the message down into parts; sender, recipient, subject, body, headers, and various types of metadata
    - Extracts URLs from message body, performing:
      - Regex matching for plaintext emails
      - HTML parsing for HTML emails
  - Downloads attachments
  - If an .eml or .msg file is attached, it parses headers from this as well

- Rapidly assembles context at machine speeds, analyzes emails from multiple perspectives, and assigns a score to each component. Any of the phases can also include a whitelist for known safe values (i.e., a score of 0) or a blacklist for known bad values (i.e., a score of 10). LogicHub performs:
  - Sender and header analysis
    - Can evaluate IPv4 and IPv6 IPs from the received elements in the header and compare against IPs flagged by threat intelligence solutions
    - Runs SPF and DMARC checks to determine spoofing likelihood
    - Scores the email when there is a positive hit for malicious IP or suspicious domain spoofing
  - Attachment analysis
    - Checks attachment hashes against threat intelligence sources and scores on a positive hit
    - Analyses attachments using an OEM ML-based analysis engine
    - Can upload attachments to a sandbox for detonation/exploration, and parse the analysis output to assign a score
  - URL investigation
    - Scores URLs with OEM threat intelligence and domain WHOIS information
    - Can check URLs against third-party tools, services, and products and score them accordingly
    - Can also score based on the similarity of URL domains against organization-specific domains (e.g., “acmicorp.com” vs “acm1corp.com”)
    - Can check additional threat databases, if specified
  - Keyword search
    - Searches the body of the email for a custom set of keywords and increases the score if any keyword is found (e.g., keywords associated with credential harvesting and malware-laced phishing emails e.g. “password” or “account number”)
  - Subject and Email Body analysis
    - LogicHub can use the results of human analysis to build and maintain a predictive (machine learning) model

- Combines the analysis results and provides a final score based on a formula or ML model.
  - A simple formula is to use the highest score from any investigation as the final score
  - A more advanced formula uses combined weighted average of all scores
  - A machine learning model bases analysis on examples provided by an analyst

- Performs response and remediation steps depending on final score. For example:
  - Threat found: Alert SOC, notify user, and create ticket for audit trail
    - Additionally, can search inboxes for other users who might have received the same malicious email and delete those emails from their inbox
  - Suspicious email: Notify SOC of need to further investigate, notify user, create ticket for tracking which includes investigation details gathered
  - No threat: Notify user that email was not malicious and create and close ticket for tracking

  Exact scores and responses can be adjusted to improve coverage and accuracy, and to account for specific situations.



The LogicHub Phishing Triage summary view enables analysts to review recent emails at a glance and discover threats associated with specific emails.

Respond to Phishing Attacks Faster

Automate Triage with 97% Accuracy	Respond with Speed and Precision	A Complete SOAR Platform	Fast Time-To-Value
Powered by Machine Learning	Workflow and Orchestration	Highly Customizable, Multi-Purpose	2 Weeks to Go Live

Real Customer Use Case

Industry	Location	Revenue	Employees
Food	US Midwest	$14.9B	10,000

Customer Problem

- More than 200 emails per day, each taking approximately 5 minutes to triage
- The number of emails per day growing faster than net new headcount
- Triage and remediation only occurring during daytime hours

LogicHub Solution

- Phishing Triage used its scoring to sort each email into one of three classes:
  - True Positive
  - Requires Human Eyes for Further Analysis
  - False Positive

  For true and false positives, users are sent an email 24x7 within 10 minutes of submitting an email for analysis.

- An audit of large samples determined LogicHub was 100% accurate with 75% coverage, saving the time equivalent of 2 full-time employees (FTEs), reducing the threat of phishing attacks, and bringing more consistency to threat analysis

Customer Quote

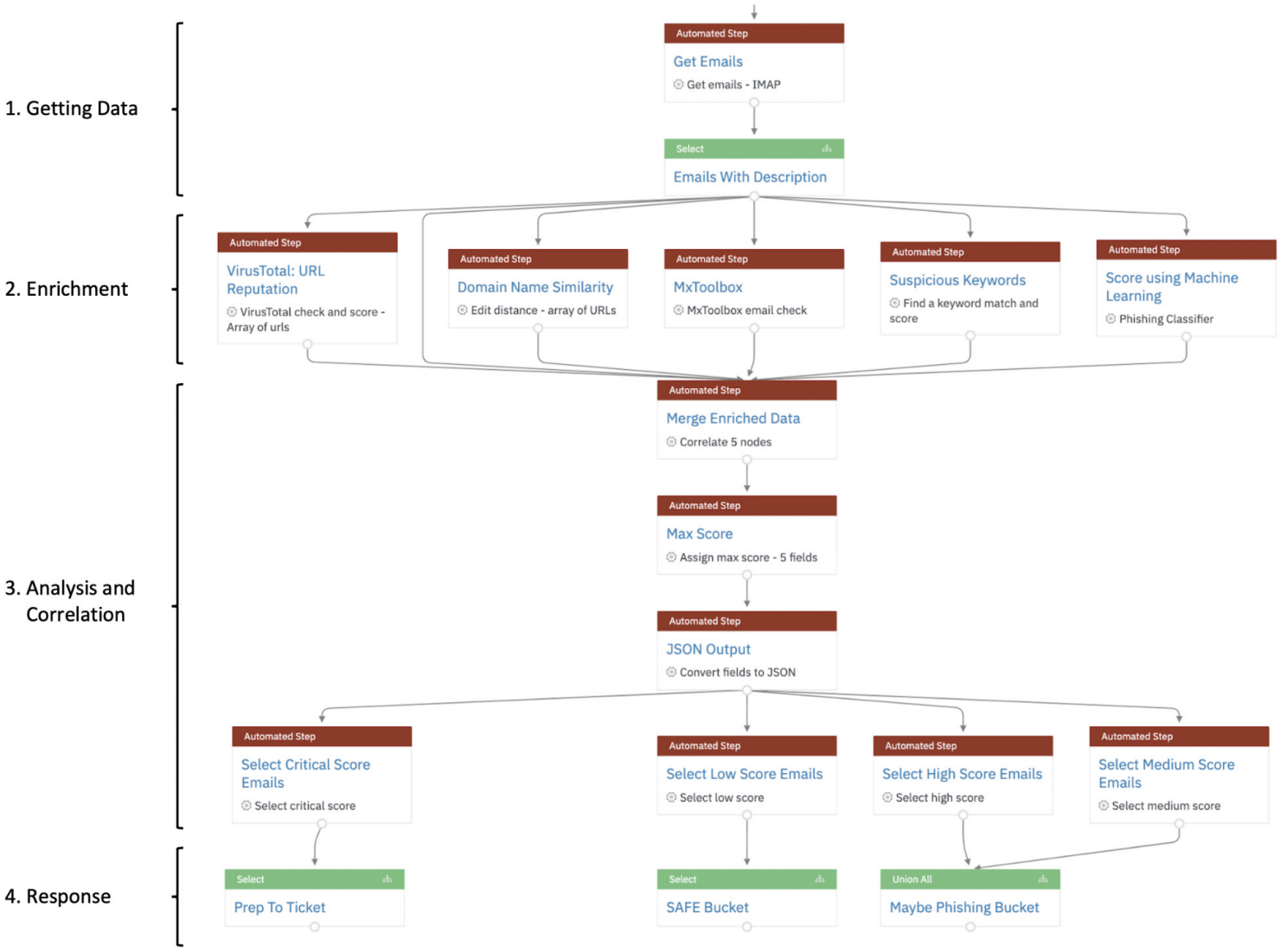
"The number of reported phishing emails continues to grow exponentially, meanwhile, my headcount has not. Using automation allows us to automate existing alerts as well as keep up with the ever rising number of new alerts."

CISO

How It Works: Advanced Phishing Email Triage Example

Building a LogicHub Flow for Email Triage

The diagram below shows an example of a customized flow for Advanced Phishing Email Triage. Working with your team, LogicHub can help you build an automation workflow for phishing email triage tailored to your particular IT environment and SOC requirements.



Step 1

GETTING THE DATA

To kick off the triage process, the flow retrieves the input data to be analyzed. In this phishing triage example, the input is a batch of emails suspected of having phishing content that are obtained from an IMAP server. For more general use cases involving alert messages, the connection can be to Splunk, Sumo Logic, or other Security Information and Event Management (SIEM) system.

Step 2 **ENRICHMENT**

The enrichment step augments the incoming emails with additional information necessary for the triage analysis.

In this case, the emails are enriched with several types of information.

Information from third party services

A LogicHub flow can call on third-party reputation services to enrich the data with information about known risks and bad actors.

In the specific example flow above, URLs embedded in the emails are extracted and queried against a reputation database, and the sender's email address is checked against an email address database.

Some examples of third-party tools that can provide enrichment include:

- Reputation databases (Anomali, ReversingLabs, VirusTotal, MxToolbox)
- IP address geolocation (Maxmind)
- Public or private malware sandbox platforms (FireEye, Cuckoo, Palo Alto Networks WildFire).
- Examination of file attachments (Hybrid Analysis, YARA rules)

LogicHub Modules

The example flow uses two LogicHub modules to enrich the email. The Domain Name Similarity module checks for the similarity between the URLs embedded in the email and the recipient's own domain. If they are too similar, such as a replacement of "e" with "ê", it might indicate that the sender is trying to spear phish by tricking the recipient into recognizing the malicious URL as a legitimate company URL.

The Keyword Matching module matches an editable list of suspicious keywords, such as "password", "verify", and "pharmacy" against the content of the email messages. If any of these words is present, the email is more likely to be a phishing email.

Machine Learning Classifiers

LogicHub allows you to incorporate machine learning at the enrichment step or for analysis and decision making. In our phishing example, how can the security analyst determine whether the user is correctly reporting spam?

Starting with a sample set of correctly classified emails, you can create a machine learning model to apply and improve predictions. Powerful LogicHub operators such as *predictLabelFromText* and *createModelFromText* allow you to start predicting how to classify other emails by assigning likelihood scores from 0 to 10. As the system learns, it becomes more and more effective at spotting the malicious phishing emails.

Analyses can also be inaccurate because of low quality or unreliable data. Suppose you are computing the maximum of multiple factors, but one of the factors is unreliable. If you don't include a mechanism to adjust for that factor, your results will suffer. A machine learning model that uses LogicHub operators such as combineScores and createScoreCombiner can help your flow adjust for inaccurate inputs.

Step 3 **ANALYSIS AND DECISION MAKING**

After the phishing emails have been brought into LogicHub and enriched with information from third party and LogicHub sources, it is time for analysis and decision making.

The flow first merges the multiple sources of enriched data using a pre-built LogicHub correlation module. A maximum score is determined based on a comparison of the correlated data.

The flow can allow a manual adjustment of the score (not shown in the diagram above) based on information that wasn't available from the enrichment sources. For example, a reputation database might have flagged a URL as suspicious, but the analyst knows that the URL is legitimate based on other information.

With the calculated and adjusted scores in hand, the emails are placed into separate classes depending on determined risk (low, medium, high, or critical).

Step 4 **OUTPUT RESPONSE**

The output of a typical LogicHub flow assigns the analyzed emails to classes according to rankings determined by the flow (0-10) and the associated actions (or lack thereof).

You can design a flow to include any number of classes and to designate an appropriate action for each class. If an alert is deemed to be a true incident, LogicHub can automate the response and remediation steps. The action for a critical alert might be to automatically block messages, whereas the action for a high alert level might be to perform additional analysis or reexamine manually. In our example flow, the analyzed alerts are placed in three classes according to low, medium & high, or critical risk. For critical alerts, a ticket is prepared for a case management system such as ServiceNow or JIRA. This option allows customers to use their own case management tools to collaborate and manage their response workflow.

The example flow incorporates one type of output response, but LogicHub offers multiple options for reporting results. Data can be sent back to a SIEM, for example, by adding a comment to a Splunk Notable and updating its status or automatically notifying the SOC. The output can also be forwarded to other tools or services that take immediate action to stop an attack. Examples include blocking a URL or blocking a file in the corporate network.

To complete the triage automation, LogicHub allows you to set a schedule for running the flow repeatedly. Each time the flow runs, it automatically processes any new data and reports results without requiring any additional input from the security analyst.

It is good practice to close the loop on emails submitted by users for analysis. By responding to these users, we let them know that their concerns are being addressed in a methodical way, that their efforts are appreciated, and that their actions are contributing to the security of the organization overall.

Summary

Automating phishing triage with LogicHub is easy and powerful. Using built-in analysis, optional third-party analysis, and customizable flows, SOCs and IT security teams can automate and accelerate phishing triage with 97% accuracy while reducing the triage workload by 75%. Most importantly, LogicHub improves security by investigating alerts in real time, removing false positives, and producing very few false negatives.

LogicHub Phishing Triage offers a clear reasoning-decision path that can be traced back when needed. This path effectively provides an explanation of each decision to the analyst. Machine Learning systems that produce explainable decisions are superior to other systems that require analysts to make final decisions themselves or to trust decisions delivered by a machine learning systems whose reasoning cannot be analyzed, explained, or manually corrected.

LogicHub is a highly customizable automation platform, allowing customers to tailor and fine tune playbooks to their liking in order to address phishing triage automation and security automation challenges such as alert triage, threat hunting, and other critical security activities that can be automated. LogicHub Phishing Triage enables SOC teams and other security experts to leverage powerful automation to beat back the ever-growing threat of phishing attacks and other email-borne risks.

About LogicHub

LogicHub is the only security automation platform that delivers autonomous detection and response automation for security operations teams. By applying machine learning and analytics on large data sets, LogicHub automates security analyst workflows and decisions, helping teams save time, find critical threats, and eliminate false positives.

LogicHub

a: 154 E Dana Street, Mountain View, CA 94041
w: www.logichub.com
e: info@logichub.com
p: (650) 262-3756