LogicHub

Solution Brief

LogicHub Phishing Alert Triage

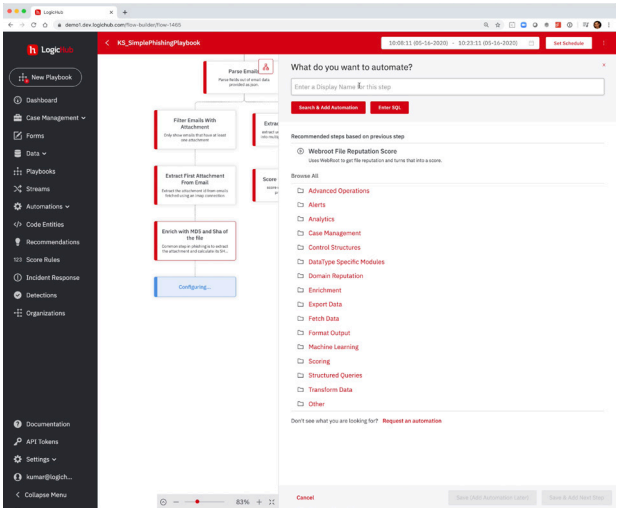
Automation-driven detection and response

Phishing is one of the most common attack techniques used by cyber criminals. It's an easy way to distribute malicious payloads or convince unsuspecting employees to link to external sites capable of distributing malware.

- **94% of malware** is delivered via email
- **22% of all data breaches** include a phishing attack
- And **phishing requires minimal effort and skill to execute**.

A skilled security analyst can identify most phishing attacks, but investigating every potential incident is a time-consuming and largely manual process. Just the time required to cut and paste data from potential phishing emails into 3rd party tools can waste critical minutes and hours every day. With LogicHub SOAR+, you can reduce the entire phishing detection, triage and response life cycle to seconds or minutes.

Automated Phishing Triage



The LogicHub Solution

LogicHub's SOAR+ platform delivers automated detection and response at scale, automatically analyzing emails to identify suspicious and malicious indicators indicating a phishing attempt. These indicators are automatically mapped to the MITRE ATT&CK framework to ensure a best practices approach. And unlike traditional SOAR platforms, which are typically limited to executing a few thousand daily tasks, LogicHub can analyze, triage and respond to millions of events and alerts per day, ensuring that nothing slips through the cracks.

LogicHub phishing playbooks automatically analyze emails to identify potential phishing attacks and triage alerts to rapidly detect true threats. It automatically executes actions that would otherwise be manual and slow, like extracting and submitting URLs and message headers to threat intelligence platforms, and sending attachments to sandbox technologies for inspection. Each email can then be rapidly assigned an accurate risk score so that analysts can stay focused on responding to and remediating true positives.

Automated Phishing Triage

Challenge: Phishing is one of the most common forms of attack in both frequency and volume. But investigating each potentially malicious email is a time consuming and repetitive process involving a series of low level tasks like cutting and pasting data from message headers and attachments into multiple platforms for threat analysis, triaging potentially malicious emails, notifying impacted users, quarantining impacted devices, opening trouble tickets and manually deleting infected files.

Solution: LogicHub has out-of-the-box templates and an intuitive builder that lets you quickly and easily create playbooks that automatically perform previously manual tasks necessary to investigate, triage and respond to phishing attacks. Every potential phishing email is automatically analyzed and any real threat is identified and responded to at machine speeds. Previously manual processes that took minutes or hours can be queued up for one-click approval or automatically executed in seconds.

LogicHub SOAR+ Benefits

With the LogicHub SOAR+platform, you can reduce the entire phishing detection, triage and response life cycle to seconds or minutes. Benefits include:

- Integration with any mail platform (MS Exchange, Gmail, O365, LDAP, etc.)
- Easy-to-use builder to create comprehensive phishing playbooks specific to any organization in minutes
- Extensive one-click and fully automated incident response actions for rapid mitigation
- Phishing attacks are automatically correlated against associated tactics and techniques from MITRE ATT&CK

How it works

1 Analyze and Investigate

Parse relevant data from email header

Send data (IP, URL, hash, etc) to threat intelligence platforms

Submit attachments to sandbox for inspection

2 Detect and Triage

Aggregate threat scores from mutliple tools

Automatically apply intelligent risk rating to assess overall threat severity

Create confirmed cases for any valid threat

3 Respond and Contain

Notify security operations team of phishing activity

Automatically correlate all associated cases

Queue one-click response actions and execute automated steps

To learn more about the LogicHub MDR+ visit: logichub.com/SOAR

LogicHub

301 N Whisman Rd Mountain View, CA 94043
info@logichub.com • tel 650- 262-3756
logichub.com