CYWARE™

## Use Case

# Unstructured Threat Intel Advisory Automation

# Digging for Indicators in Unstructured Data

Threat intelligence acts as a catalyst in combating advanced threat actors through insights on their tactics, techniques, and procedures (TTPs). Organizations often consume threat intelligence from industry peers, independent threat hunters, or regulatory bodies on a daily basis. Such intelligence usually comes in the form of an email, report, or a blog post and is called unstructured threat data. It is often a cumbersome process for security analysts to analyze and incorporate this unstructured threat intel data in their workflow. This is where security automation comes into play.

# Bringing Structure with Automation

To improve the analysis of potential threats, security teams can leverage security automation to automatically extract various threat indicators and attack patterns from unstructured documents.

**The threat intelligence advisory playbook performs the following tasks:**

### Extraction of Threat Indicators

The playbook automatically parses relevant indicators like IP, Domains, URLs, Hashes, etc. from the unstructured data.

### Enrichment and Analysis

The collected IOCs are enriched internally and externally with information from several trusted intel sources including Cyware Threat Intelligence eXchange (CTIX) and other trusted threat intel sources and the final Risk Score is calculated. The playbook performs the following actions to prioritize the actioning on relevant intelligence:

- The threat intelligence is filtered based on a customizable confidence score mechanism (Cyware Confidence Score) which is calculated from factors that include threat sightings, TLP, Source of intelligence, and more.

- The intel is then automatically correlated with the threat intelligence Watchlist of the deployed SIEM solution.

- The IOCs Reputation is checked via several trusted intelligence sources.

## Response Actions

**Based on the triaging information several response actions are performed such as:**

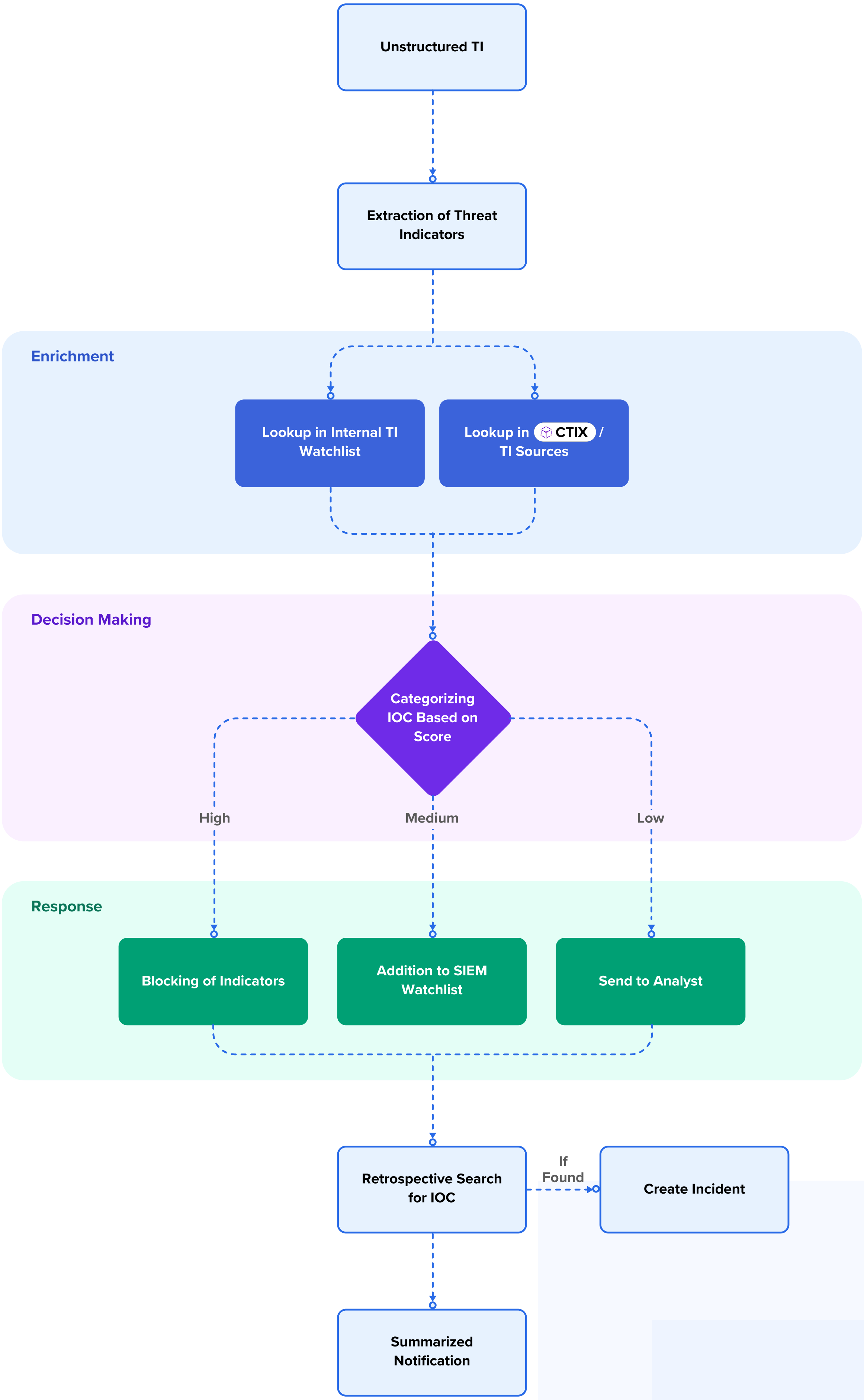
- Blocking of indicators on Firewall, Proxy, EDR, etc. as a preventive measure.
- Addition of the indicator to the watchlist of SIEM solution, UEBA, NBAD, etc.

## Retrospective Search

Based on the criticality of the indicators, a retrospective search is performed to identify any observation of the IOCs within the environment.

## Summarized Internal Notification:

Once all the actions are performed on the reported intelligence advisory, an email notification with the original advisory and information on all related actions taken is sent to respective stakeholders responsible for managing the security operations as well as compliance.


Unstructured TI
Extraction of Threat Indicators
Enrichment
Lookup in Internal TI Watchlist
Lookup in CTIX / TI Sources
Decision Making
Categorizing IOC Based on Score
High
Medium
Low
Response
Blocking of Indicators
Addition to SIEM Watchlist
Send to Analyst
Retrospective Search for IOC
If Found
Create Incident
Summarized Notification

# Cyware Advantage

## Format-Agnostic Normalization

CTIX provides a unique capability to ingest threat information in a variety of unstructured formats and custom formats and convert into STIX 1.x, STIX 2.0, or STIX 2.1 collections with a single click.

## Faster Decision Making

After processing unstructured threat intel, the Rules Engine of CTIX enables security teams to take automated actions to respond to and prevent any potential threats within the early stages of the cyber kill chain.

## Reduce Analyst Workload

While security analysts are already burdened with processing hundreds or thousands of threat alerts, the use of security automation helps reduce the workload by accelerating the analysis of unstructured threat information.

CYWARE™

228 Park Ave S #77147 New York,
New York 10003-1502

cyware.com | sales@cyware.com

☎ 855-MY-CYWARE