CYWARE™

Use Case

Automated Threat Intelligence Enrichment

So Many Indicators...

Threat intelligence enrichment is a critical component of any incident or threat investigation process. The enrichment process helps remove false-positives and deduce actionable intelligence for threat response and other security operations. Until now, the process has largely been manual with intel analysts sifting through several trusted sources and enriching indicators manually. The process is cumbersome, takes up a lot of time, and is impractical in the present security scenario where hundreds if not thousands of indicators are collected on a daily basis. However, with Cyware's automation solution, the enrichment process can be performed within seconds along with high-level analysis.

One Playbook to Enrich them All

With the threat intelligence enrichment playbook, indicators will automatically be enriched with more details and context to improve incident investigation with the **Cyware Fusion and Threat Response (CFTR)** and **Cyware Orchestrate**. The playbook will be triggered for any indicator of compromise (IOC) observation during an incident investigation.

The threat intelligence enrichment playbook performs the following tasks:

Indicator Ingestion

The playbook automatically ingests and normalizes indicators from external and internal threat intelligence.

Extraction and Enrichment

The playbook enriches the collected IOCs from several internal and external trusted intel sources and the final Risk Score is calculated. Following actions help to prioritize the actioning on relevant intel:

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

• The indicator reputation scores are collected across several trusted intel enrichment sources.

• Automated correlation with Threat Intel Watchlist of SIEM solution.

•Contextual information about the IOCs and their relevance with other malware, threat campaigns, or indicators is collected

Indicator Scoring

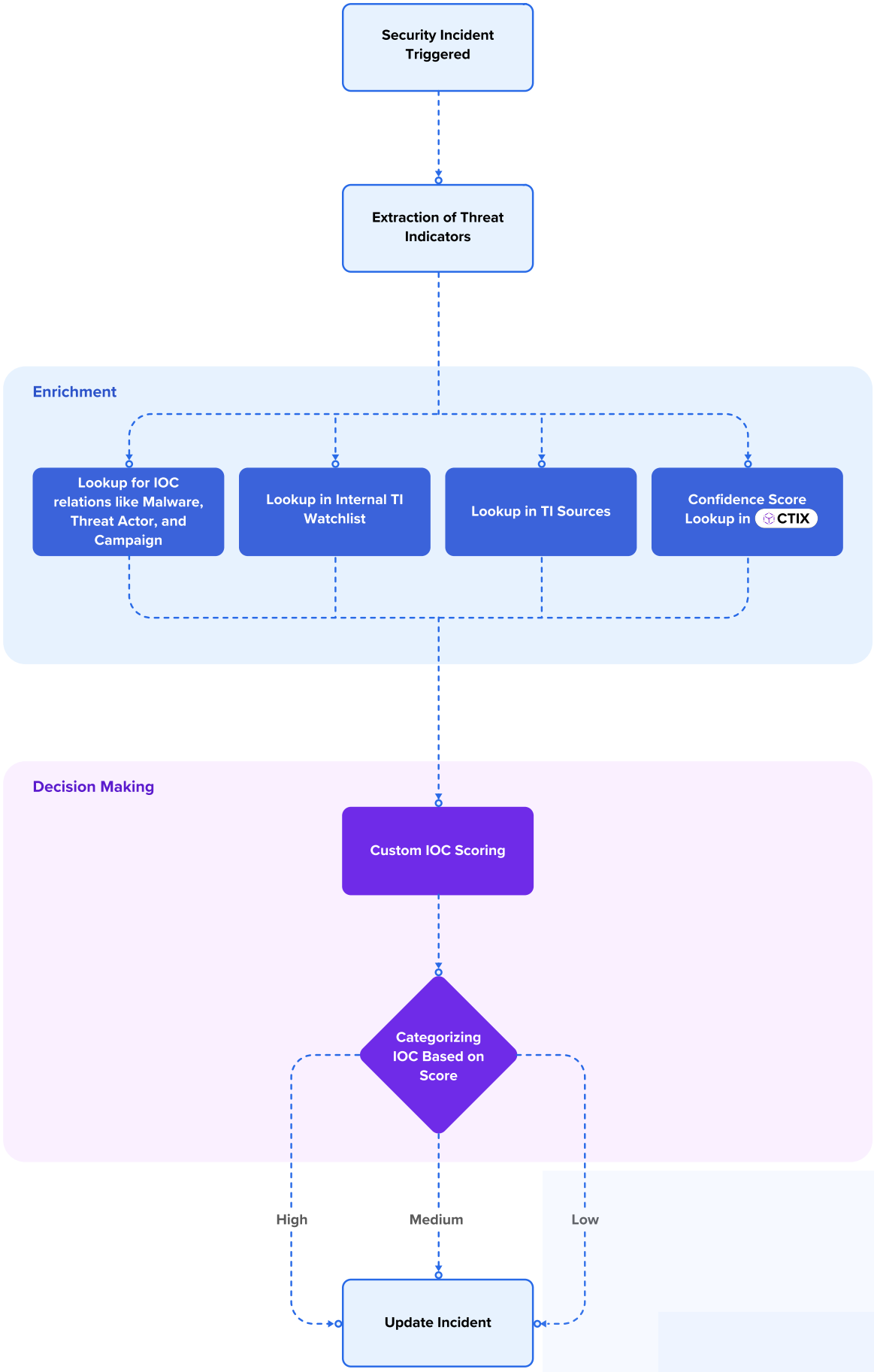
Following the enrichment process, the defined custom logic in playbooks can automatically score the intel and help prioritize the next course of response action for the incident.

Analysis and Action Taking

Based on the triaging information several response actions can be triggered

•Blocking of indicators on Firewall, EDR, etc as a preventive measure.

•Adding the indicator to the watchlist of the SIEM solution.


Security Incident Triggered
Extraction of Threat Indicators
Enrichment
Lookup for IOC relations like Malware, Threat Actor, and Campaign
Lookup in Internal TI Watchlist
Lookup in TI Sources
Confidence Score Lookup in CTIX
Decision Making
Custom IOC Scoring
Categorizing IOC Based on Score
High
Medium
Low
Update Incident

Cyware Advantage

Automate Repeatable Tasks

With the automated process of sifting relevant IOCs, analysts save significant time that can be better spent on in-depth analysis and strategic action.

Actionable Threat Intelligence

With the automated enrichment and scoring of indicators based on contextual factors, the playbook provides actionable intel for security analysts to work upon.

Better Response Workflow

The automated playbook provides SOC analysts with a comprehensive view of the response workflow, equipping them with correlation intelligence for informed decision making.

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

cyware.com | sales@cyware.com

855-MY-CYWARE