Use Case

Automated Threat Intelligence Enrichment
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.

So Many Indicators...

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 Security Orchestration Layer (CSOL). 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:
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.

**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.
Automated Threat Intelligence Enrichment
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.