Use Case Definition

This document provides a template for defining a use case to be implemented in XSOAR TIM. The Use Case is defined by the process, logic, and tasks that are being done as part of the Threat Intelligence Lifecycle.

Use Case Definition

Use Case Name ●Name of Use Case ●Example - Blocking Malicious Indicators of Compromise, Allowlist Office 365	
Collection ●Which threat intelligence feeds and enrichments are required? ●Example - Collect phishing related indicators from Cofense, or collect command and control IP Addresses from abuse.ch.	
Indicator fields and mapping ●Indicator fields that are required as part of the collection process ●Example: Any custom fields which are not included out of the box. Example, internal references.	
Enrichment ●Enriching of IOCs from thread intel, or from internal sources ●Example: Enriching URLs and IP addresses from cloud threat intel services, enriching event with raw data	
Analysis & Processing of Indicators ●Using playbooks, analyze indicators from feeds. ●Example: Enrichment of indicators, lookup indicators against internal IP ranges, business partners, push indicators to SIEM based on criteria.	
Operationalize ●Integrate indicators into SIEM / FireWall / EDR / etc. ●Push indicators to ArcSight or QRadar using playbooks. Host an external dynamic list using Palo Alto Networks PAN-OS EDL Service	

3rd Party Integrations

Product Category Type of product	**Product name and version** Exact product name and version	**Actions needed** Reference logic steps above

Indicator Structure (Custom Field)

Field name Malware Family	**Field Type** Short Text	**Comments and Values**	**Layout Placement** Indicator Details / Indicator Quickview