Cortex XSOAR Content Pack Design Document - [Your Company]

Introduction

Hello and thank you for your willingness to contribute to the Cortex XSOAR ecosystem. This Design Document is meant to help you define the structure and requirements of your Cortex XSOAR Content Pack and make sure that is aligned with our best practices.

If you don't know what a Cortex XSOAR Content Pack is or our requirements, please review our Cortex XSOAR Developer Hub at xsoar.pan.dev to get started. Make sure to check out the concepts section.

How to complete this document

Please complete as many sections as possible, since some of them may not be relevant to your use case or pack structure.
This Document is required prior to beginning the build phase of your contribution.

A good example to use as a reference on how to fill in this document is the HELLO WORLD Content Pack design: here

Help & Support

Any question about this document or partner integrations can be answered in:
DFIR Slack community on any of the public channels here
Or by mail to: soar.alliances@paloaltonetworks.com

Resources and Background

To start creating your own contribution it is important to understand some basic concepts and how XSOAR works.
XSOAR Developer Hub can be found here:https://xsoar.pan.dev/docs/welcome
The most important things to understand before starting designing and developing are:

- Getting started guide with all the links to the relevant information such as:
  - Concepts
  - FAQ
  - Product training
  - DFIR Slack channel
  - Recommended tools
  - More relevant information
- **Design tutorial** - here
- Enablement videos of the whole building a pack process - here

General Information

Document Author (Partner)	
Document Reviewer (Palo Alto Networks)	

Partner Information

Product Information

Each Pack should integrate with one product. Provide details about your product

Product Name	
Description	
Supported Version(s)	
Notes	

Team and Contacts

Name	**Email**	**Title**	**Role (BD/Tech)**

Content Pack General Details

Content Pack Details

Company Name	[Your Company]
Partner ID*	[your_partner_id]
Content Pack Name	
Content Pack Support Email	
Content Pack Product URL	

* The Partner ID can be found in an email sent from our system. Search for emails you've received with the subject line "Hello Cortex XSOAR Developer"

Content Pack Metadata

General metadata information
https://xsoar.pan.dev/docs/packs/packs-format#pack_metadatajson
Information about description, use cases, keywords, tags and categories
https://xsoar.pan.dev/docs/documentation/pack-docs

XSOAR Minimum Version	6.5
Content Pack Version *(major.minor.revision)*	1.0.0
Pack Description	[Add freely]
Pack Use Cases	[From list in the link above]
Pack Keywords	[Add freely]
Pack Tags	[From list in the link above]
Pack Categories	[From list in the link above]

Use Cases

Please provide a general overview of the Use Cases you are going to implement in this Content Pack. See our documentation for more information.

Use Case	Description

Pack Content

XSOAR components - please read the links to get more information about each component.
A content pack must have at least one of the entities

Entity Type	**Name(s)**
Integrations	
Classifiers and Mappers	
Playbooks	
Incidents Types	
Indicators	
Automations (Scripts)	
Widgets & Dashboards	
Other	

If you have Integration as part of your pack, see the next page.

Integrations

Usually each content pack contains one integration, in case your pack includes more than one, you must replicate this section for every integration.
Please read about the fetching incidents/indicator feed options in the link below.

Integration Name (PascalCase)	
Integration Description	
Minimum XSOAR version	6.5
Fetches incidents? *(Yes/No)*	
(only if fetches incidents) **What Incident types does it support?**	
(only if fetches incidents) ***What filters does it support? (i.e. severity, priority, etc.)***	
Indicator Feed? *(Yes/No)*	No
(only if indicator feed) **What Indicator types it supports?**	
Supports mirroring? *(Yes/No)*	No
(only if implements mirroring) **What mirroring capabilities does it support (select all that apply)?** ● **Inbound** ● **Outbound** ● **Mapping**	

Integration Parameters

Please fill in the parameters that your integration supports.

- ***Connectivity Parameters**: include all necessary parameters to allow an integration to connect to your Product API, such as **URL**, **API Key**, etc: these parameters depend on your product/API (i.e. some products use username/password instead of API keys). Note that **proxy** and **insecure** are required and should not be removed.*

- ***Fetch Parameters**: if your integration supports fetching incidents, you should provide all the parameters needed to successfully work, such as maximum incidents to fetch per time, first fetch and all the filters. Additional common filters are **severity** and **type**, but they vary depending on your Product and its API. Note that **isFetch** and **incidentType** are required for integrations that fetch incidents and should not be removed.*

You can also check out the Hello World example as a reference.

*Supported parameter types are: **Short Text, Long Text, Boolean, Encrypted, Single Select, Multi Select.***

Connectivity Parameters

Parameter name	**Type**	**Required** *(Yes/No)*	**Default Value**	**Description**
proxy	Boolean	Yes	False	Whether to use XSOAR’s system proxy settings to connect to the API.
insecure	Boolean	Yes	False	Whether to allow connections without verifying SSL certificates validity.
url	Short Text	Yes		The FQDN/IP the integration should connect to.
apiKey	Encrypted	Yes		The API Key required to authenticate to the service.

Fetch Incidents Parameters

Parameter name	**Type**	**Required** *(Yes/No)*	**Default Value**	**Description**
isFetch	Boolean	Yes	No	Enable fetch incidents
incidentType	Single-Select	No	None	Incident type to map if no classifier is provided.
maxIncidents		Yes	20	Maximum

				number of incidents to fetch every time.
firstFetch	Short Text	No	2 weeks	Date or relative timestamp to start fetching incidents from.
severity	Multi-Select	No	High,Critical	Severity levels of the alerts to fetch from the third party API (that will generate incidents in Cortex XSOAR).
alertType	Multi-Select	No	All	Type(s) of alerts to fetch from the third party API.

Integration Commands

Use this section to provide information about the commands that are supported by your integration: the name, a brief description of what they do, the list of their arguments and whether they are reputation commands (that are commands that return a reputation about a specific indicator type, such as !ip, !domain, !url, !cve), use the following naming convention for commands: PRODUCTNAME-OBJECTNAME-ACTION

Command Name	**Description**	**Arguments** *(comma separated)*	**Reputation command?** *(Yes/No)*	**Output Path**

Every command that needs to save results to context, should have outputs - read more here.
A very easy way to create outputs is using **demisto-sdk** command with the **generate-outputs** flag, read about it here

Classifiers and Mappers

*If your Content Pack includes integration(s), and they provide a **fetch incidents** functionality, it is recommended to provide at least one Incident Type in your Pack, and either a Classifier or a Mapper to help customers work with the incidents that your integration fetches. If your integration(s) provide the **fetch indicators** functionality (aka it is a feed integration), it is also recommended to provide Classifiers and Mappers for the Indicator Types you support (either out of the box ones, or custom). More details here.*

Classifier(s) names	
(only if the integration fetches incidents) **Supported Incident Types**	
(only if the integration feeds indicators) **Supported Indicator types**	
Mapper(s) names	

Incidents Fields

If you are including custom Incident Fields and Layouts in your Content Pack, please list all the elements and dependencies here. More details here, here and here.
***It is recommended to use built-in XSOAR incident fields**. Only if needed you should consider adding new fields.*

*The following table should list all the custom Incident Fields and where they are used. Supported Incident Field types are: **Attachments, Boolean, Date Picker, Grid (table), HTML, Long Text, Markdown, Multi-select, Number, Role, Short Text, Single-select, Tags, Timer/SLA, URL, User.***

Incident Field Name	**Incident Field Type**	**Used In** *(Incident Types)*	**Used In** *(Layout, if custom)*

Indicators Fields

If you are including custom Indicator Types, Fields and Layouts in your Content Pack, please list all the elements and dependencies here.

The following table lists all the custom Indicator Fields and where they are used. Supported Indicator Field types are: ***Boolean, Date Picker, Grid (table), Long Text, Markdown, Multi-select, Number, Role, Short Text, Single-select, Tags, URL, User.***

Indicator Field Name	**Indicator Field Type**	**Used In** *(Indicator Types)*	**Used In** *(Layout, if custom)*

Playbooks

Fill in the following table the required information for each playbook that is part of the content pack (excluding the test playbook).
Playbook overview, task types, inputs and outputs

Playbook Name	
Description *(What it does)*	
Triggers *(What triggers the incident - Incident Types, Feed, Sub-playbook)*	
Steps (*The main steps and decisions that are part of the playbook)*	
Inputs *(comma separated list of the Inputs that this Playbook supports.)*	
Outputs (output the playbook returns)	
Dependencies *(optional)*	

Scripts (Automations)

If your Content Pack includes Scripts (aka Automations), fill in the table below with general details of the scripts and what capabilities they provide. Fill in the Tags cells only if your scripts serve specific purposes that require them (i.e. Transformers, Dynamic Layout Sections, etc).

Script Name	**Description**	**Arguments** *(comma separated)*	**Tags** *(comma separated)*

Widgets and Dashboards

Brief description here

Widget Name	**Widget Type**	**Widget Description**	**Used In (Dashboard(s))**

Dashboard Name	**Description**