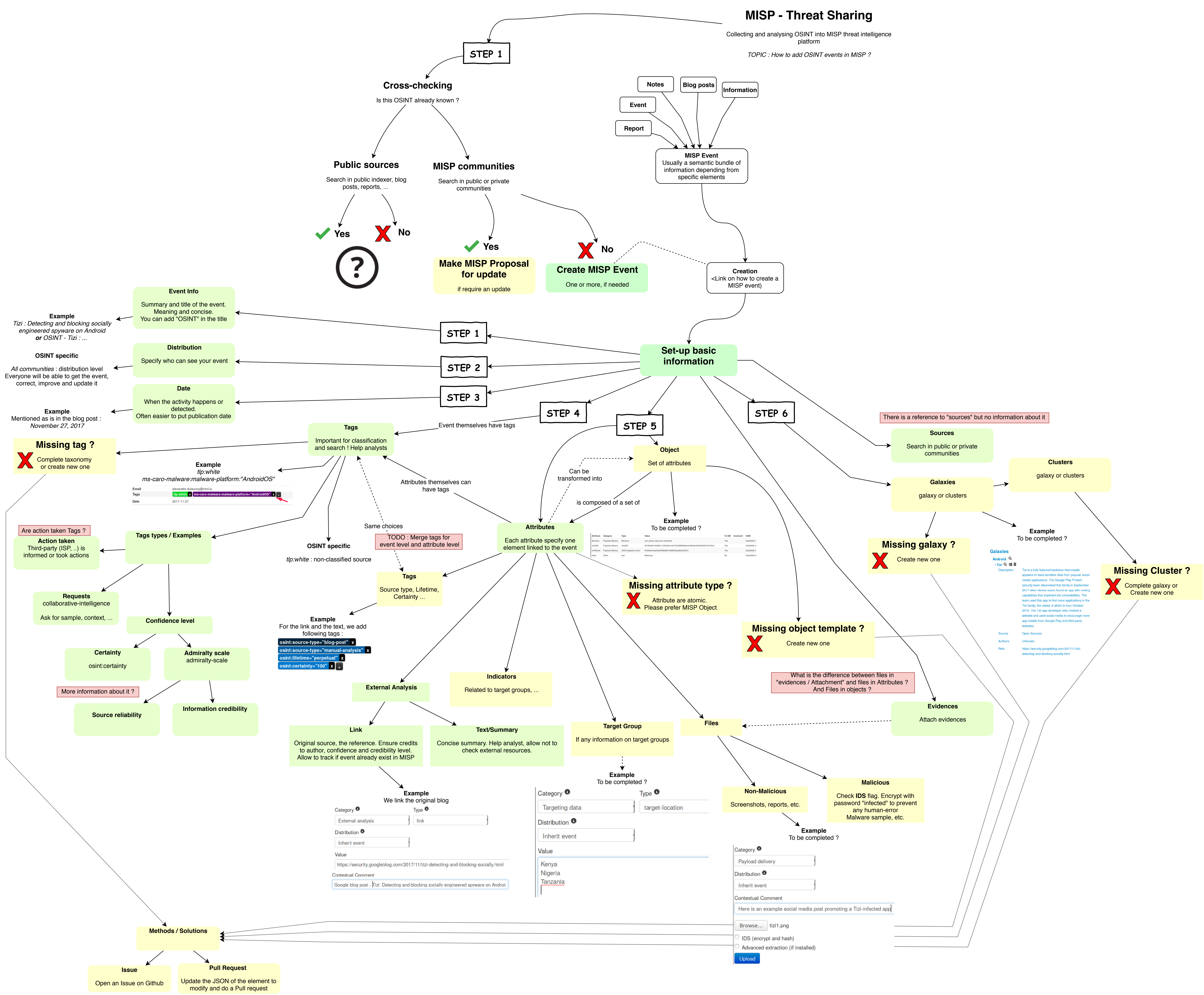
MISP - Threat Sharing
Collecting and analysing OSINT into MISP threat intelligence platform
TOPIC : How to add OSINT events in MISP ?
STEP 1
Cross-checking
Is this OSINT already known ?
Public sources
Search in public indexer, blog posts, reports, ...
Yes
No
MISP communities
Search in public or private communities
Yes
Make MISP Proposal for update
if require an update
No
Create MISP Event
One or more, if needed
Notes
Blog posts
Information
Event
Report
MISP Event
Usually a semantic bundle of information depending from specific elements
Creation
<Link on how to create a MISP event)
Set-up basic information
STEP 1
Event Info
Summary and title of the event. Meaning and concise. You can add "OSINT" in the title
Example
Tizi : Detecting and blocking socially engineered spyware on Android or OSINT - Tizi : ...
STEP 2
Distribution
Specify who can see your event
OSINT specific
All communities : distribution level Everyone will be able to get the event, correct, improve and update it
STEP 3
Date
When the activity happens or detected. Often easier to put publication date
Example
Mentioned as is in the blog post : November 27, 2017
STEP 4
Event themselves have tags
Tags
Important for classification and search ! Help analysts
Missing tag ?
Complete taxonomy or create new one
Example
tlp:white
ms-caro-malware:malware-platform:"AndroidOS"
Are action taken Tags ?
Action taken
Third-party (ISP, ..) is informed or took actions
Tags types / Examples
Requests
collaborative-intelligence
Ask for sample, context, ...
Confidence level
Certainty
osint:certainty
Admiralty scale
admiralty-scale
More information about it ?
Source reliability
Information credibility
OSINT specific
tlp:white : non-classified source
Same choices
TODO : Merge tags for event level and attribute level
Attributes themselves can have tags
Tags
Source type, Lifetime, Certainty ...
Example
For the link and the text, we add following tags :
osint:source-type="blog-post"
osint:source-type="manual-analysis"
osint:lifetime="perpetual"
osint:certainty="100"
STEP 5
Object
Set of attributes
Can be transformed into
is composed of a set of
Example
To be completed ?
Attributes
Each attribute specify one element linked to the event
Missing attribute type ?
Attribute are atomic. Please prefer MISP Object
Missing object template ?
Create new one
External Analysis
Link
Original source, the reference. Ensure credits to author, confidence and credibility level. Allow to track if event already exist in MISP
Example
We link the original blog
Category
External analysis
Type
link
Distribution
Inherit event
Value
https://security.googleblog.com/2017/11/tizi-detecting-and-blocking-socially.html
Contextual Comment
Google blog post - Tizi: Detecting and blocking socially engineered spyware on Androi
Text/Summary
Concise summary. Help analyst, allow not to check external resources.
Indicators
Related to target groups, ...
Target Group
If any information on target groups
Example
To be completed ?
Category
Targeting data
Type
target-location
Distribution
Inherit event
Value
Kenya
Nigeria
Tanzania
Files
Non-Malicious
Screenshots, reports, etc.
Malicious
Check IDS flag. Encrypt with password "infected" to prevent any human-error Malware sample, etc.
Example
To be completed ?
Category
Payload delivery
Distribution
Inherit event
Contextual Comment
Here is an example social media post promoting a Tizi-infected app
Browse...
tizi1.png
IDS (encrypt and hash)
Advanced extraction (if installed)
Upload
What is the difference between files in "evidences / Attachment" and files in Attributes ? And Files in objects ?
Evidences
Attach evidences
STEP 6
There is a reference to "sources" but no information about it
Sources
Search in public or private communities
Clusters
galaxy or clusters
Galaxies
galaxy or clusters
Missing galaxy ?
Create new one
Example
To be completed ?
Missing Cluster ?
Complete galaxy or Create new one
Methods / Solutions
Issue
Open an Issue on Github
Pull Request
Update the JSON of the element to modify and do a Pull request