MISP User Training - General usage of MISP 2.4

MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Andras Iklody - *TLP:WHITE*

MISP Workshop @SWITCH
20161206

MISP - VM

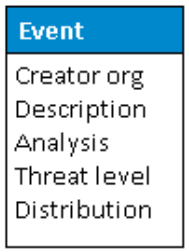
- Credentials
  - MISP admin: admin@misp.training/Password1234
  - MISP user: user@misp.training/Password1234
  - SSH: misp/Password1234
  - Mysql: root/Password1234 - misp/Password1234
- 2 network interfaces
  - NAT
  - Host only adapter
- Start the enrichment system by typing:
  - cd /home/misp/misp-modules/bin
  - python3 misp-modules.py

MISP - General Usage

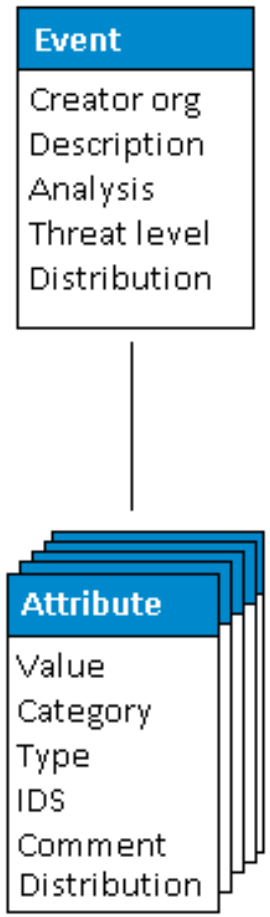
Plan for this part of the training

- Data model
- Viewing data
- Creating data
- Co-operation
- Distribution
- Exports

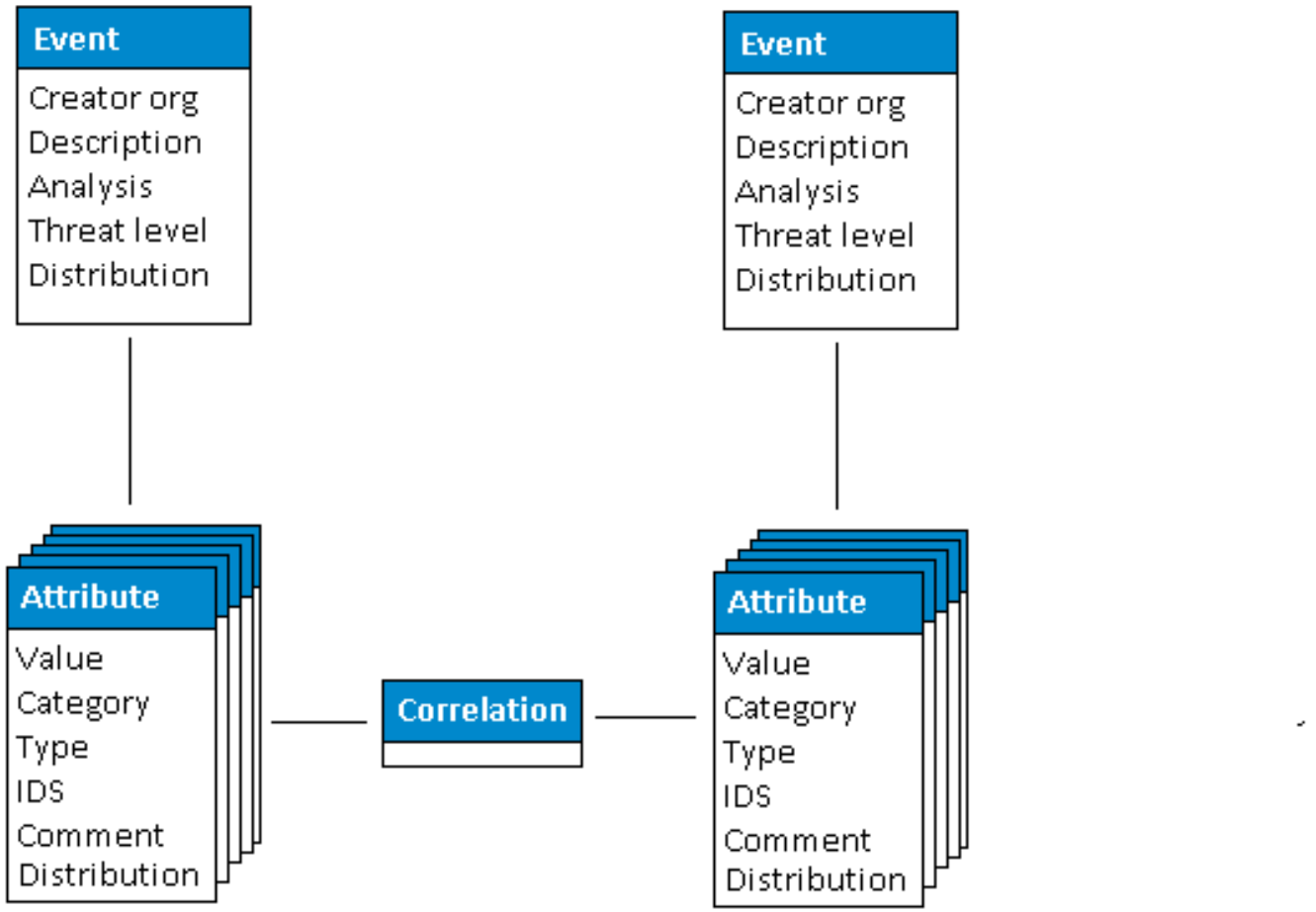
MISP - Event (MISP's basic building block)



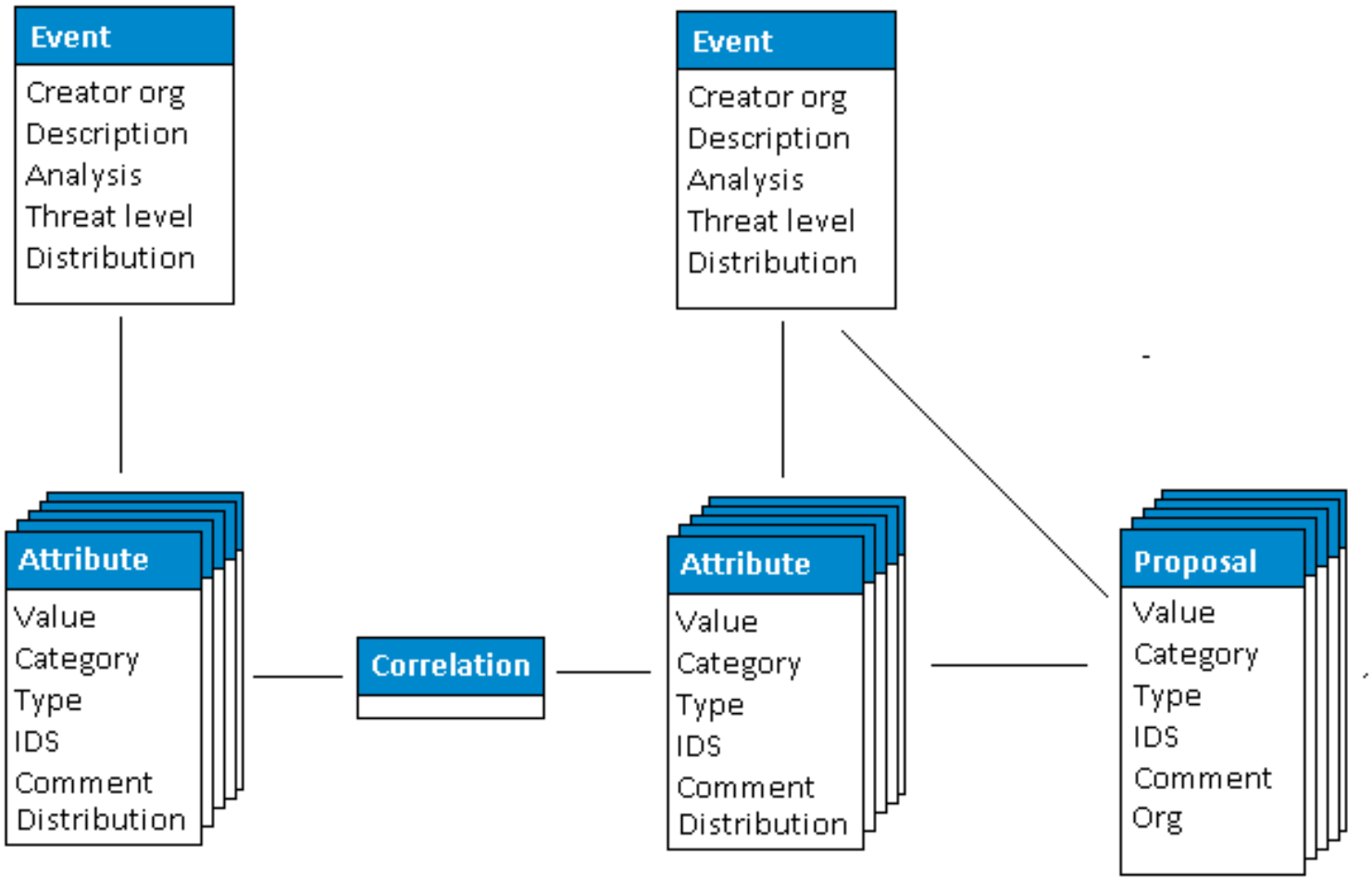
MISP - Event (Attributes, giving meaning to events)



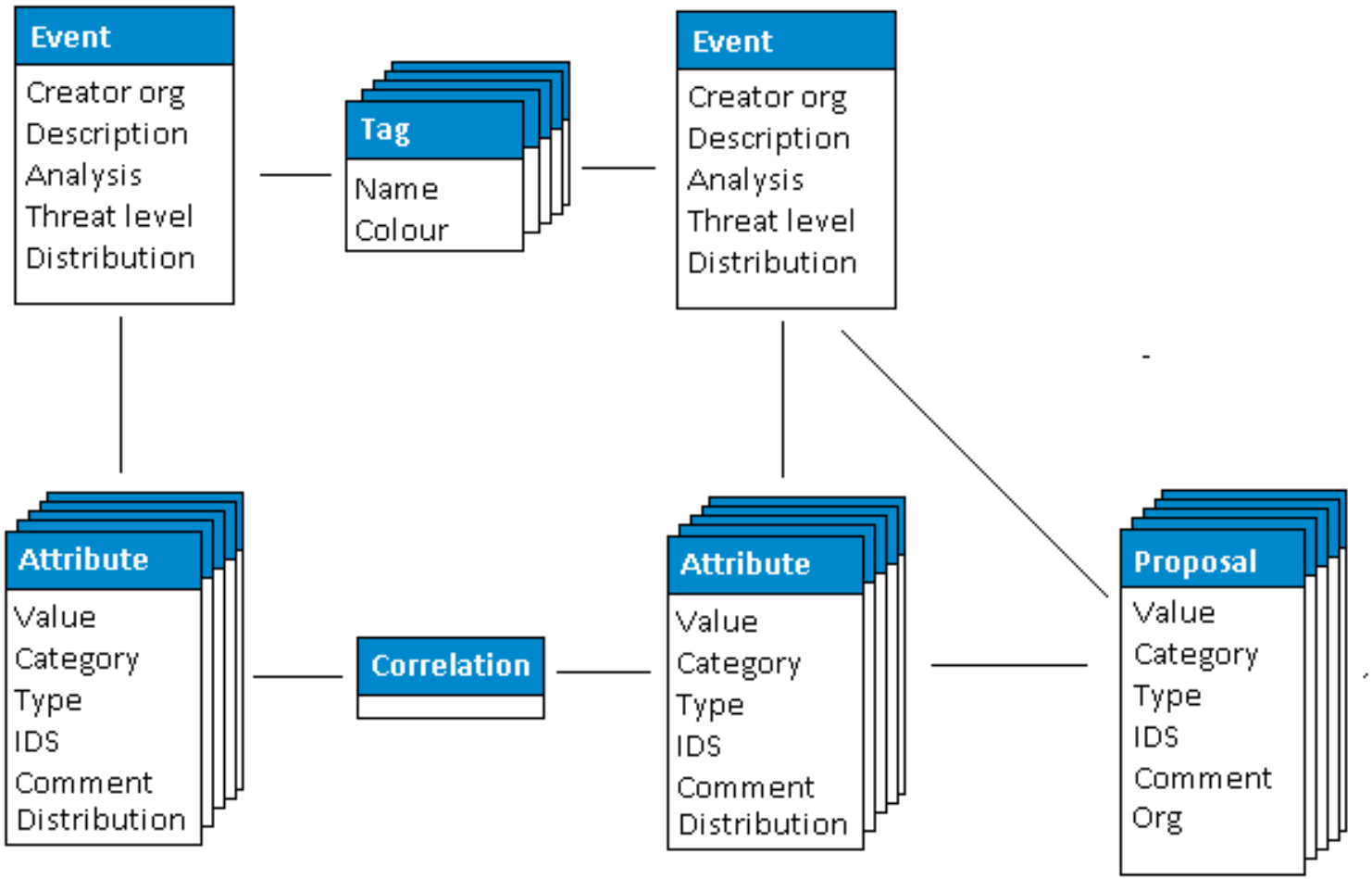
MISP - Event (Correlations on similar attributes)



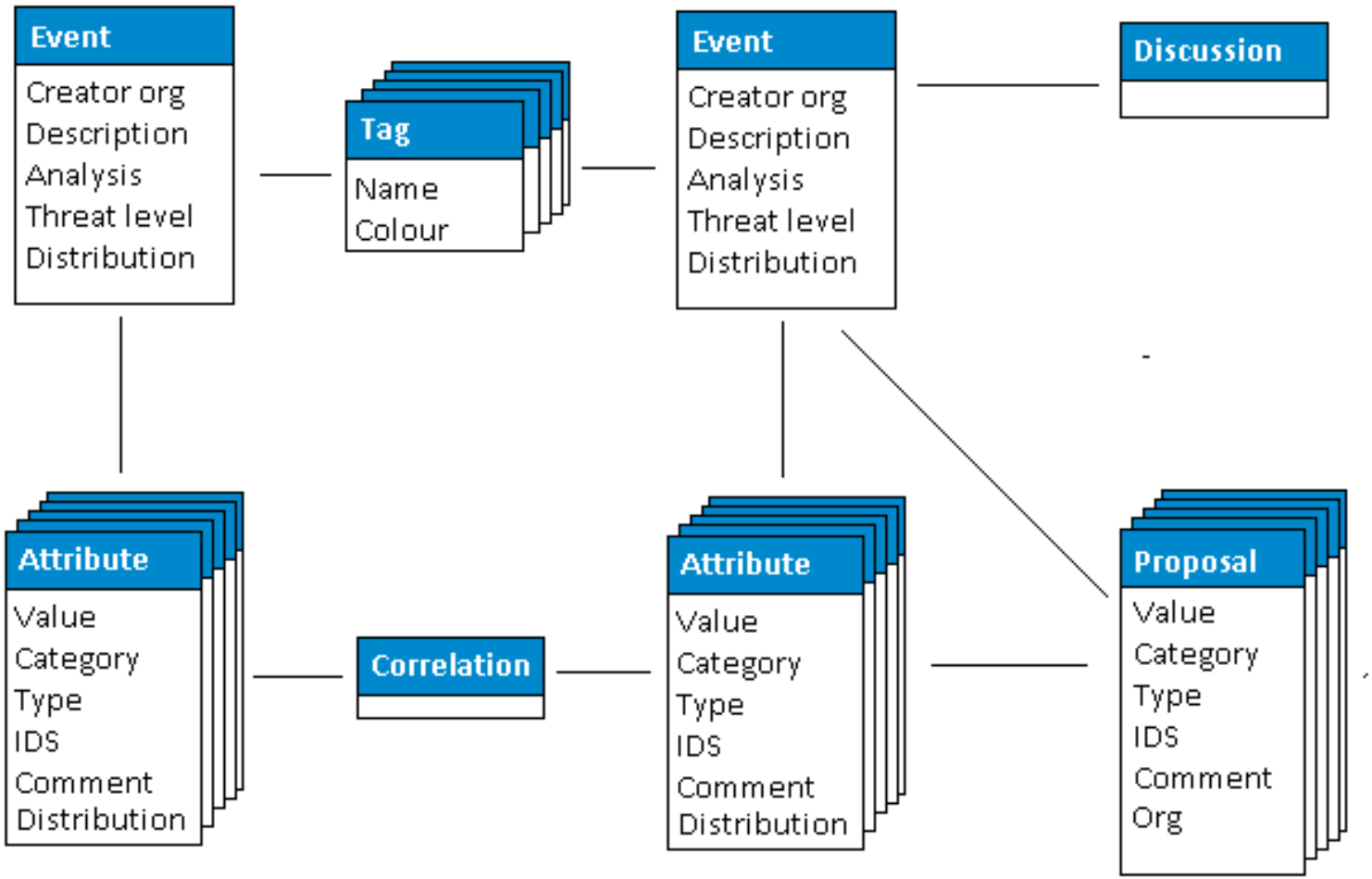
MISP - Event (Proposals)



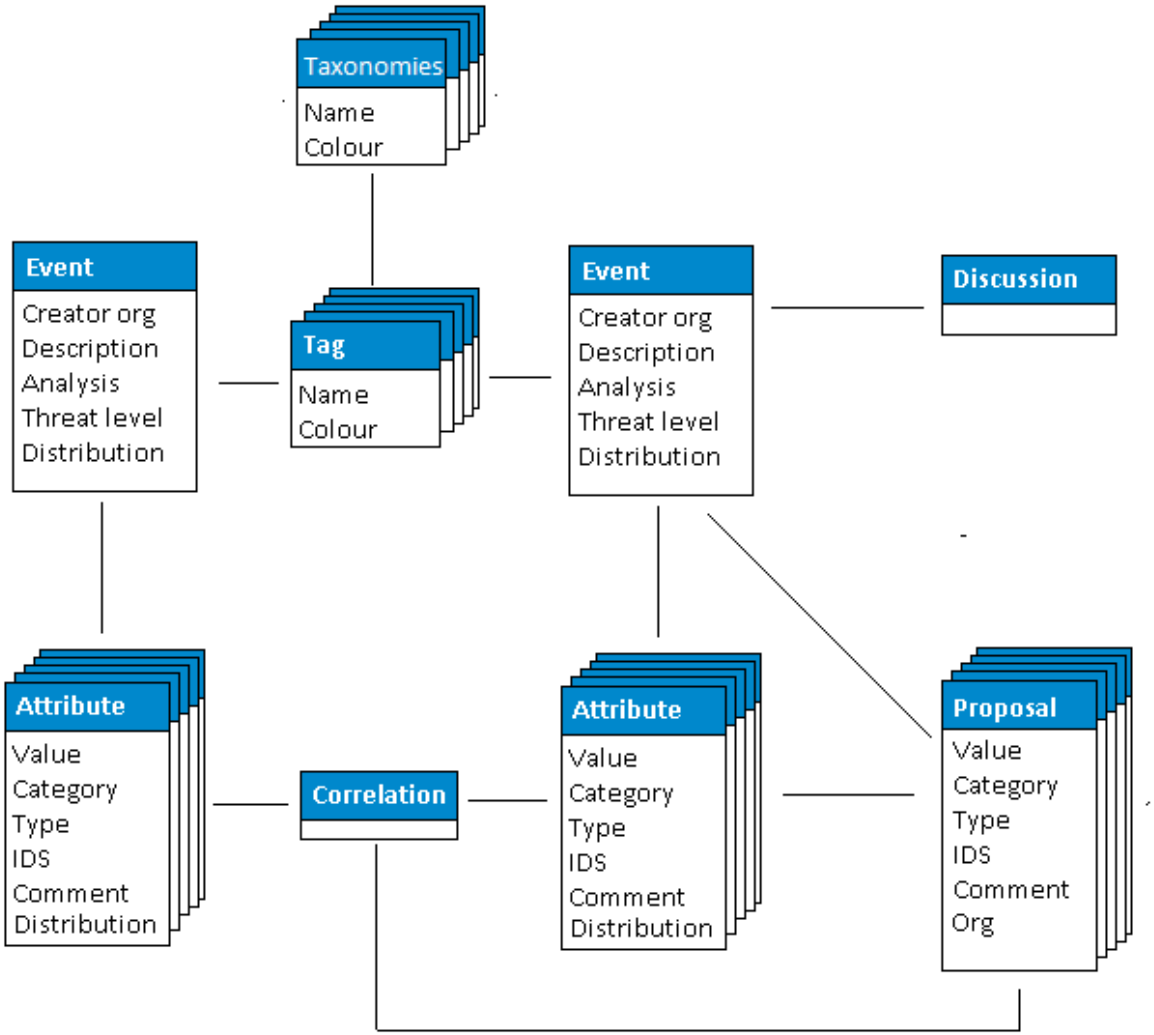
MISP - Event (Tags)



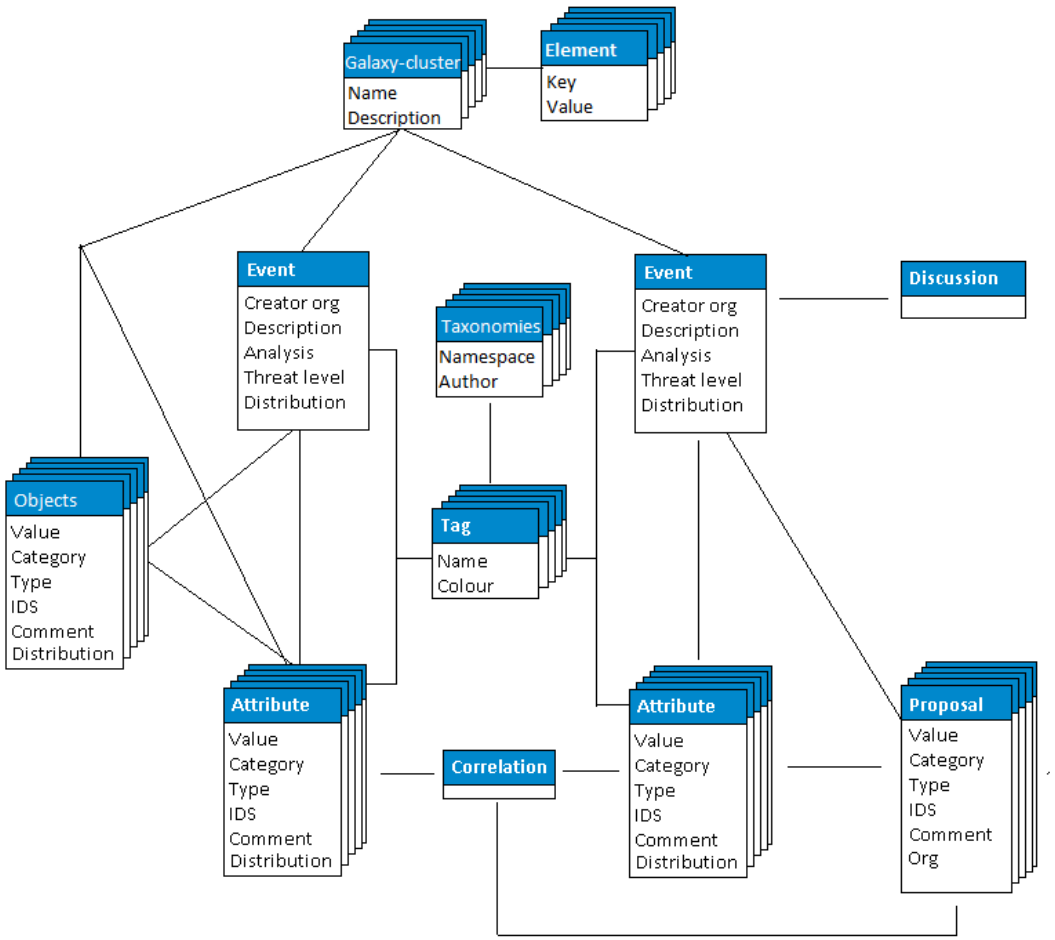
MISP - Event (Discussions)



MISP - Event (Taxonomies and proposal correlations)



MISP - Event (The Future of MISP's datamodel)



MISP - Viewing the Event Index

- Event Index
  - Event context
  - Tags
  - Distribution
  - Correlations
- Filters

MISP - Viewing an Event

- Event View
  - Event context
  - Attributes
    - Category/type
    - IDS
    - Correlations
  - Proposals
  - Discussions
- Tools to find what you are looking for

MISP - Creating an event (exercise1)

Fill out the Event metadata fields

- Info: Malicious file beaconing
- Date: 2016-03-22
- Analysis: Initial
- Threat Level: Low
- Distribution: This Community only

MISP - Creating an event (exercise1)

- Add Attributes to the event
  - Network activity/hostname: download.microsoft.com
  - Network activity/ip-dst: 208.91.198.130
  - Malware-sample: verybad.exe
  - Artifact dropped/filename: C:\Users\dropped_file.txt
  - Look at regex table
- Get IP address using enrichment for download.microsoft.com
- Notice the correlation

MISP - Creating an event using the freetext import tool (exercise2)

- Fill out the Event metadata fields
  - Info: Duqu 2.0 - IOCs
  - Date: 2016-03-22
  - Analysis: Complete
  - Tag: Type:OSINT, Duqu
  - Threat Level: High
  - Distribution: All

MISP - Creating an event (exercise2)

- Add Attributes to the event using the freetext import tool
- Use the sample report provided (duqu-report.txt)
- Look for other events tagged Duqu

MISP - Creating an event using the templates (exercise3)

Fill out the Event metadata fields

- Info: Phishing e-mail
- Date: 2016-03-22
- Analysis: Complete
- Tag: phishing and scam from the circl Taxonomy, also TLP:Green
- Threat Level: Low
- Distribution: All

MISP - Creating an event (exercise3)

Add Attributes using the Phishing e-mail template

- From address: perspirating-madman@microsoft.com
- Malicious url: http://windows.microsoft.com/en-us/internet-explorer/download-ie
- Email subject: Download IE today, we support HTML5 now!
- Source IP: 23.96.52.53

MISP - Collaboration (exercise4)

- Propose a change to an attribute
  - In Event 9 attribute with IP 79.98.112.35 is causing false positives
  - Suggest to set IDS off
  - Explain your reasoning in the discussions
- Normally contacting by e-mail through MISP is another option

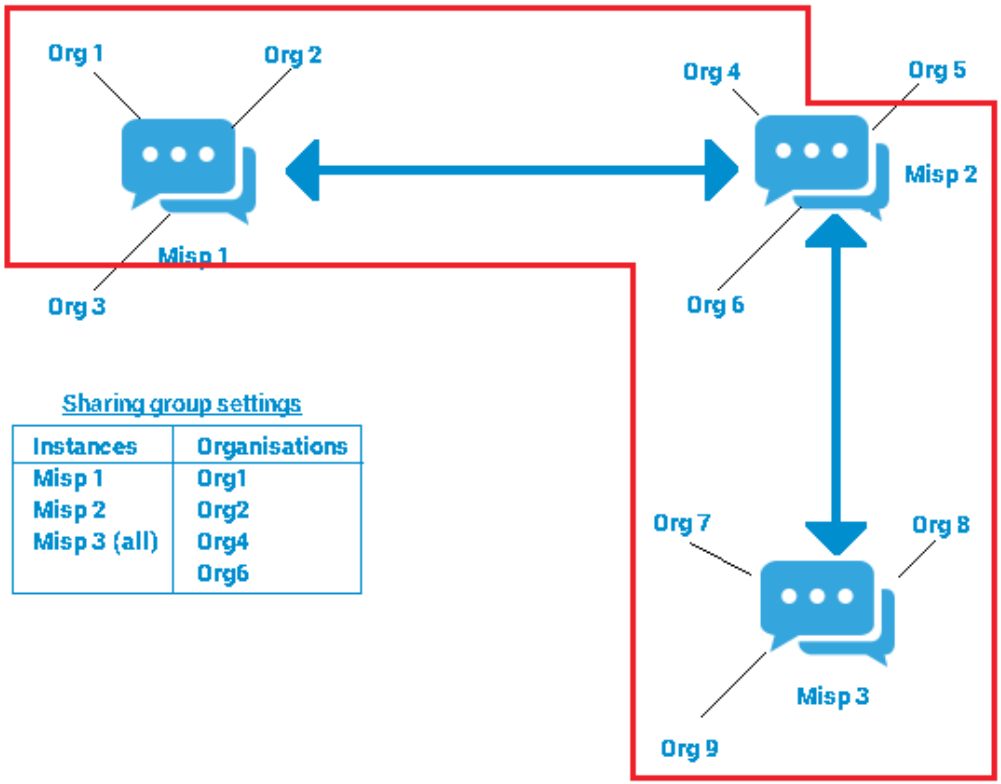
MISP - Delegation (exercise4)

- Create an event
  - Distribution: Your organisation only
  - Info: "Test event"
  - Attribute: Network-activity/ip-dst: 85.25.194.116
  - Attribute: Network-activity/ip-dst: 192.168.1.10
- Delegate publishing to CIRCL

MISP - Distributions explained

- Your Organisation Only
- This Community Only
- Connected Communities
- All Communities
- Sharing Group

MISP - Distribution and Topology



Sharing group settings

Instances	Organisations
Misp 1	Org1
Misp 2	Org2
Misp 3 (all)	Org4
	Org6

MISP - Exports and API

- Download an event
- Quick glance at the APIs
- Download search results
- Cached exports