
# Ce1sus: A Contribution to an Improved Cyber Threat Intelligence Handling

June 2015

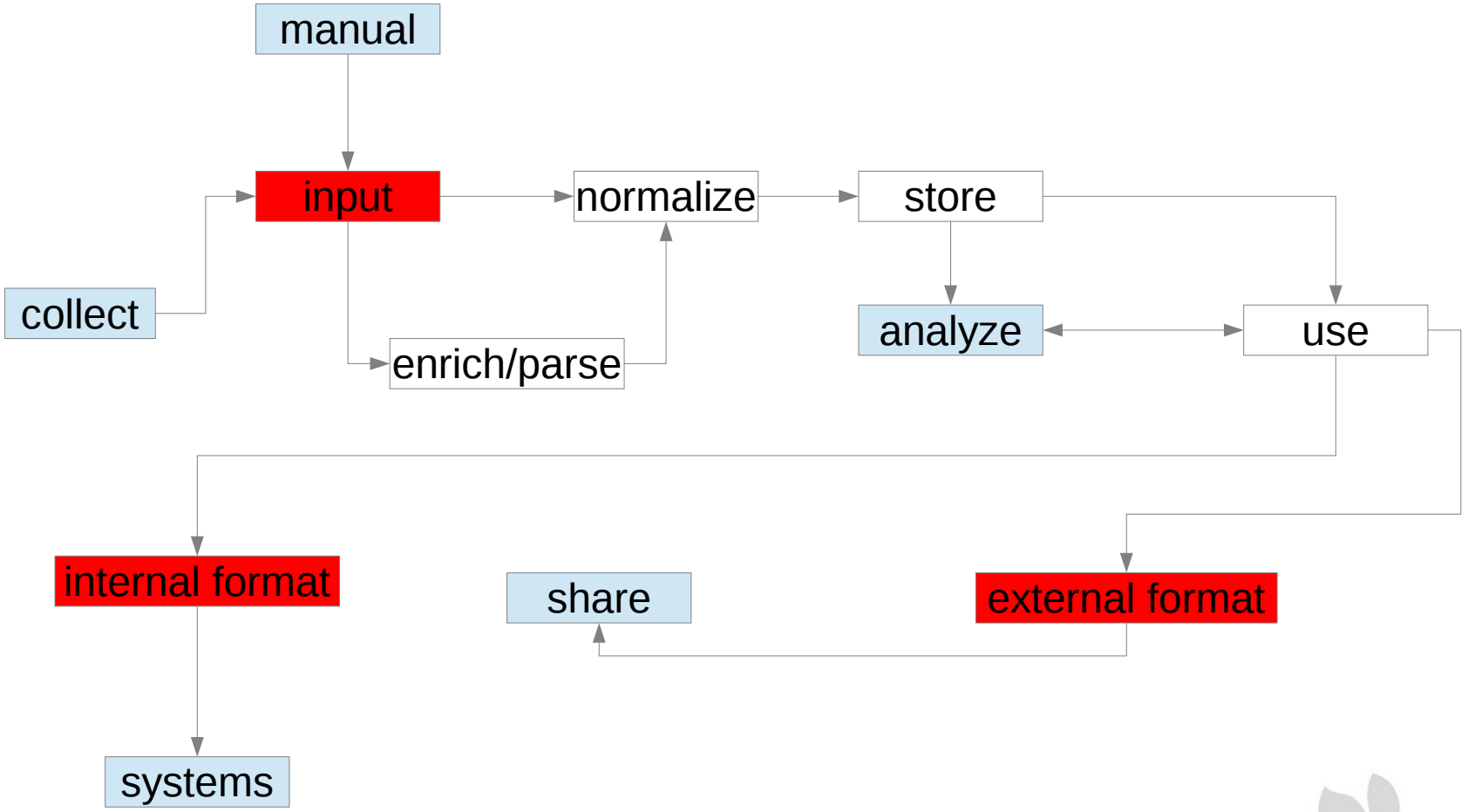
LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

CERT gouvernemental

# Requirements

- Ease of use
- Structured data
  - Output
  - Work-flow of the threat
- Interoperability
  - Combine it with existing tools
- Automated data enrichment/parsing

# Data work-flow




red

light blue

# Structure example

**Email**
- sender: max@ups.com
- subject: UPS delivery
- body
- ….

**File**
- hashes
  - 19dc4d6061d1e1e57255f08692d3ea92
- type (dropper)
- size: 356B
- name: delivery.doc

**URI**
- url: http://194.123.123.11/f.zip

**Address**
- ipv4: 194.123.123.11

**File**
- hashes
  - 00349d3191033a12caaa76c7c95ff12b
- type (trojan)
- size: 123B
- name: a.com

**URI**
- url: http://example.com/image.png

**Domain**
- Domain name: example.com

**Address**
- ipv4: 128.55.11.2

# Structure example

**Email**
- sender: max@ups.com
- subject: UPS delivery
- body
- ….

**File**
- hashes
  - 19dc4d6061d1e1e57255f08692d3ea92
- type (dropper)
- size: 356B
- name: delivery.doc

**URI**
- url: http://194.123.123.11/f.zip

**Address**
- ipv4: 194.123.123.11

**File**
- hashes
  - 00349d3191033a12caaa76c7c95ff12b
- type (trojan)
- size: 123B
- name: a.com

**URI**
- url: http://example.com/image.png

**Domain**
- Domain name: example.com

**Address**
- ipv4: 128.55.11.2

# Structure example

**Email**
- sender: max@ups.com
- subject: UPS delivery
- body
- ….

**File**
- hashes
  - 19dc4d6061d1e1e57255f08692d3ea92
- type (dropper)
- size: 356B
- name: delivery.doc

**URI**
- url: http://194.123.123.11/f.zip

**Address**
- ipv4: 194.123.123.11

**File**
- hashes
  - 00349d3191033a12caaa76c7c95ff12b
- type (trojan)
- size: 123B
- name: a.com

**URI**
- url: http://example.com/image.png

**Domain**
- Domain name: example.com

**Address**
- ipv4: 128.55.11.2

# Benefits of such structure

- Store known informations
- Easy determination what happened
- Find patterns in threats
  - i.e. reuse of the same file
- Find more about the relations between threats

# Existing tools

- MANTIS
  - https://github.com/siemens/django-mantis
- MISP
  - https://github.com/MISP/MISP
- SOLTRA – Edge
  - https://soltraedge.com
- CRITS
- And many more

# Existing “standards”

- IODEF
- OpenIOC
- CybOX
- STIX/TAXII
- MAEC
- DAF
- And many more

# Existing “standards”

- IODEF
- OpenIOC
- CybOX
- STIX/TAXII
- MAEC
- DAF
- And many more

# ce1sus

Add new Observable

View Mode

## Observables

MaliciousEmail

MaliciousEmail

email - a505eb08-5fb7-4189-baf5-9b9aca237c70

| S | Type | Value | IOC | Options |
|---|---|---|---|---|
| | email_from | max@ups.com | | |
| | email_subject | UPS delivery | | |

File - e4d23093-6acd-4da7-a25f-ff96acb1d4e2

| S | Type | Value | IOC | Options |
|---|---|---|---|---|
| | hash_md5 | 19dc4d6061d1e1e57255f08692d3ea92 | | |
| | Size_In_Bytes | 356 | | |

URI - 3c7c25b5-27b4-4c28-bb07-3357e95ad52d

| S | Type | Value | IOC | Options |
|---|---|---|---|---|
| | url | http://194.123.123.11/f.zip | | |

Address - fb5b406e-d246-41e7-ae3f-fdcc17f8ca70

| S | Type | Value | IOC | Options |
|---|---|---|---|---|
| | ipv4_addr | 194.123.123.11 | | |

# ce1sus - features

- Structured threat (Storing and presenting)
- STIX/CybOX compatible
- Completely RESTful
- Attribute handlers
- Compatible with different formats
- Different levels of sharing

# Attribute definitions

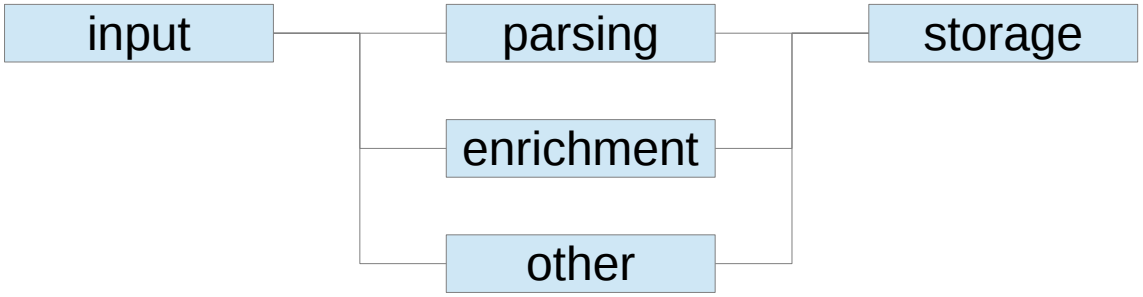
## Attribute details:

| | |
|---|---|
| **Identifier** | aa1f2e5f-9f70-4e6a-8a10-25d93fbc1581 |
| **Name** | ipv4_addr |
| **CHKSUM** | ec7c309b5451170e4b41b3aa5e3a9b24afbccc40 |
| **Description** | The IPv4-addr value specifies an IPV4 address. |
| **Regex** | ^\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}$ |
| **Data type** | String |
| **Input handler** | MultipleGenericHandler |
| **Base type** | None |
| **Default Condition** | Equals |
| **Options** | **Relationable:** ☑ |
| | **Default Shareable** ☑ |

Edit Delete

# Handlers

- A handler processes the input
  - It can decompose the data
  - Enrich the data



# Handlers and value types

## Value types

- Text
- String
- Date
- Numbers

## Handlers

- Generic handler
- Text handler
- Multiple line handler
- Combo-box handler
- Date handler
- RT and CVE handler
- File handlers
- Emailhandler
- ….

# Some other things

- Support of MISP Synchronization
- Completely open source
  - https://github.com/GOVCERT-LU/ce1sus
- There is more!! :)
  - Don't hesitate to ask me


# Thank you for your attention

jean-paul.weber@govcert.etat.lu

# Questions?