

MISP Collaboration & Sharing

Rapid-Fire of Features



Rapid-Fire of Features: Collaboration & Sharing

Time to get serious
about collaboration!



Sightings

Data ownership

Publishing

Sharing Group
Blueprints

Delegation

Extended Events

Proposals

Deletion

Analyst Data

Sharing Group

Collections




Isolation



Withholding
Information

Data Ownership

Organisation CIRCL


















ID	15
UUID	55f6ea5e-2c60-40e5-964f-47a8950d210f
Local or remote	Local
Description	CIRCL is the CERT (Computer Emergency Response Team/ Computer Security Incident Response Team) for the private sector, communes and non-governmental entities in Luxembourg.
Created by	Unknown
Creation time	2023-09-29 06:47:38
Last modified	2023-09-29 06:47:38

Members Events Sharing Groups


















Users index

< previous next >

ID	Org	Role	Email				NIDS SID	Last Login	Created	Last API Access	Actions
631	 admin		andras.iklody@circl.lu	x	x	x	4276767	✓	Never	x	   
634	 admin		sami.mokaddem@circl.lu	x	x	x	4411663	✓	Never	x	   
638	 admin		christian.studer@circl.lu	x	x	x	2012380	✓	Never	x	   

Malware distribution via GitHub issues

(complete)

Event ID	58
UUID	c44d7fd4-ac43-4fd6-a895-a1c87bb49896   
Creator org	 CIRCL
Owner org	 CIRCL
Creator user	andras.iklody@circl.lu
Published Event	 Event is in unpublished mode
Tags	                 
Date	2024-09-04
Event Level	7 Critical
Analysis	Initial

- Events belong to an Organisation
- All users from that Org. can edit it
 - (If they have the permission)

- Creator org (orgc) = Who **originally created** the Event
- Owner org (org) = Who **has control** over the Event



Proposals

<input type="checkbox"/>	2022-03-24	8d6...bef		Payload delivery	ip-src	194.78.89.250	 	 	IP address of the scammer collected from the RDP log file	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/> Inherit	   (3/0/0)	   
<input type="checkbox"/>	2024-09-05	8d6...bef	<u>ORNAME</u>	Payload delivery	ip-src	194.78.89.250			IP address of the scammer collected from the RDP log file			No		<input checked="" type="checkbox"/> 

- Proposals latch on Attributes
- Original Event creator (orgc) can either *Accept* or *Discard* it
- Proposals are synchronized


Extended Events



Successful Scam call involving money transfer

Event ID	23
UUID	53d2f469-9f7f-4e40-8dc1-a721f1b223fb  
Creator org	Training
Owner org	ORGNAME
Creator user	admin@admin.test

- Extending an Event **creates a new Event** for your Organisation
- Allows a **combined view** of both Events
- Enables **adding information** for competitive or complementary analysis













Add Event

Date Distribution 

Threat Level  Analysis 



Event Info

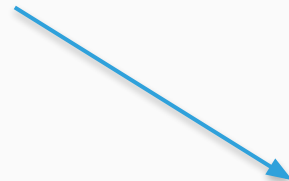
Extends Event



Matched event
ID: 23
Analysis: Completed
Threat level: Low
Tags:
 workflow:state="complete"  tip:green
 veris:action:hacking:vector="Desktop sharing"
 veris:action:social:variety="Scam"
 veris:action:social:vector="Phone"
 veris:actor:external:motive="Financial"
 veris:impact:loss:rating="Minor"
 veris:impact:loss:variety="Asset and fraud"
 social-engineering-attack-vectors:non-technical="technical-expert"
 social-engineering-attack-vectors:technical="vishing"
 misp-galaxy:mitre-attack-pattern="Phishing - T1566"
 misp-galaxy:mitre-attack-pattern="User Execution - T1204"

Info: Successful Scam call involving money transfer

Publishing

Publish Event	Date	2024-09-05
Publish (no email)	Threat Level	Low
Contact Reporter	Analysis	Completed
Download as...	Distribution	All communities  
Add Event to Collection	Published	No
	Attributes	411 (26 changed)



Distribution	All communities	 
Published	Yes	2024-09-05 09:17:39

- Sends notification emails (or not)
- Exposes IoCs to some export formats (Suricata, Bro, ...)
- Starts the synchronisation process

Analyst Data

The screenshot displays a user interface for 'Analyst Data'. At the top, there are three tabs: 'Notes & Opinions' (3 items), 'Outbound Relationships' (1 item), and 'Inbound Relationships' (0 items). Below the tabs, there are three filter buttons: 'All notes', 'Organisation notes', and 'Non-Org notes'. The main content area shows a list of notes and opinions. The first note is titled 'Note to an event' and is from 'alexandre.dulaunoy@circl.lu' 2 months ago. Below it, there is an opinion with a 'Strongly Disagree' rating of 0/100. The second note is also from 'alexandre.dulaunoy@circl.lu' 2 months ago, and it has a 'Strongly Agree' rating of 90/100. The opinion text for the second note is 'Very good report, I strongly agree with the conclusion.'

Note on Event

Opinion on Note

Opinion on Event

- Can be attached on many elements
 - Events, Attributes, Objects, Reports, Clusters, Analyst Data, Organisations, ...
- Are synchronized
- Are a light discussion and feedback mechanism

Sightings

Sightings

  
(3/0/0)

Add Sighting

Type

Source

Sighting Date

Sighting



honeypot, IDS sensor id, SIEM,...

2024-09-05

09:29:50

Sighting

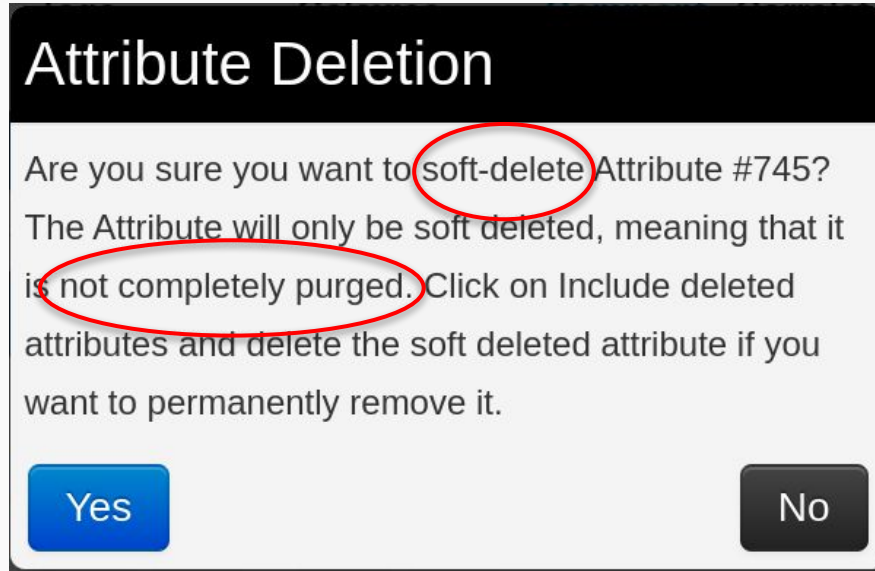
False-positive

Expiration

Add

- Enables feedback on sighted IoCs or timed false positives
- Lowest barrier of entry way for contribution
- Main use is for IoC life-cycle management

Deletion












- Soft-deletion is similar to setting a **revocation flag**
- *“You cannot remove an email from somebody else’s mailbox”*
 - MISIP has a mitigation mechanism (sanitisation) if information was leaked

Sharing Groups

- Enable **controlled sharing** for a **collection of Organisations**
- Typical use-cases:
 - List all members of a community
 - For coordinating incident response among involved parties
 - For distributing vulnerability to relevant stakeholders
 - ...

Sharing Group Organisations with even number

ID	1															
UUID	29fcd775-7296-4e06-a69f-7ae4c0c59616															
Name	Organisations with even number															
Releasability	The training organisations having an even number															
Description																
Selectable	✓															
Created by	ORGNAME															
Events	0 events															
Organisations	<table><thead><tr><th>Name</th><th>Is local</th><th>Can extend</th></tr></thead><tbody><tr><td>ORGNAME</td><td>✓</td><td>✓</td></tr><tr><td> ORG_2</td><td>✓</td><td>✗</td></tr><tr><td> ORG_4</td><td>✓</td><td>✗</td></tr><tr><td> ORG_6</td><td>✓</td><td>✗</td></tr></tbody></table>	Name	Is local	Can extend	ORGNAME	✓	✓	 ORG_2	✓	✗	 ORG_4	✓	✗	 ORG_6	✓	✗
Name	Is local	Can extend														
ORGNAME	✓	✓														
 ORG_2	✓	✗														
 ORG_4	✓	✗														
 ORG_6	✓	✗														

Sharing Group Blueprints

- Streamlines Sharing Group management

Allow to generate a Sharing Group out of:

- All organisations present in sharing group 127
- Any organisation that has *“Financial”* as its type
- But excluding any of the specifically negated countries' organisations

```
#19: Non-sanctioned financial organisations {
  "AND": {
    "OR": {
      "org_sector": "Financial",
      "sharing_group_id": 127
    },
    "NOT": {
      "org_nationality": [
        "Russia",
        "Russian Federation",
        "Belarus",
        "Republic of Belarus"
      ]
    }
  }
}
```

Collections

Collection view

ID	1
UUID	e3f571c2-f733-490d-99b4-09dad44235be
Creator org	ORGNAM
Owner org	ORGNAM
Created	2024-09-05 09:58:59
Modified	2024-09-05 09:58:59
Name	Cross-Sector Incident
Description	
Distribution	This community only

[Collection elements](#)

« previous next »

Enter value to search

Id	UUID	Element	Element type	Description	Actions
1	4b8ae643-8b47-4b87-bd48-58a1aa19c302	Event (dc5c09fe-985f-4249-ac0a-f0de8753d840)	Event		
2	8903ec3c-9b53-4284-8a06-839d8dc9dab3	Event (53d2f469-9f7f-4e40-8dc1-a721f1b223fb)	Event		

Page 1 of 1, showing 2 records out of 2 total, starting on record 1, ending on 2

- Organises data shared by the community
- Collections can be shared with organisation on the **same** MISP instance

Final words

Listen up! Here's why you need to collaborate and share threat-intel

- First off, you dominate the field by **leveraging multiple data sources**
- Next, you boost efficiency by **cutting out redundant efforts**
- Finally, you fortify your position with the **strength of the community**

