MISP- Malware Information Sharing Platform & Threat Sharing

- AYESHA BINTE MOSTOFA (1805062)
- SUMONTA NANDY AMIT (1805069)

Introduction

MISP is an open-source threat intelligence platform designed to help organizations collect, share, and analyze information about cyber threats.

It was developed to facilitate the exchange of structured threat information between organizations, including government agencies, cybersecurity researchers, and private sector entities.

Key Features

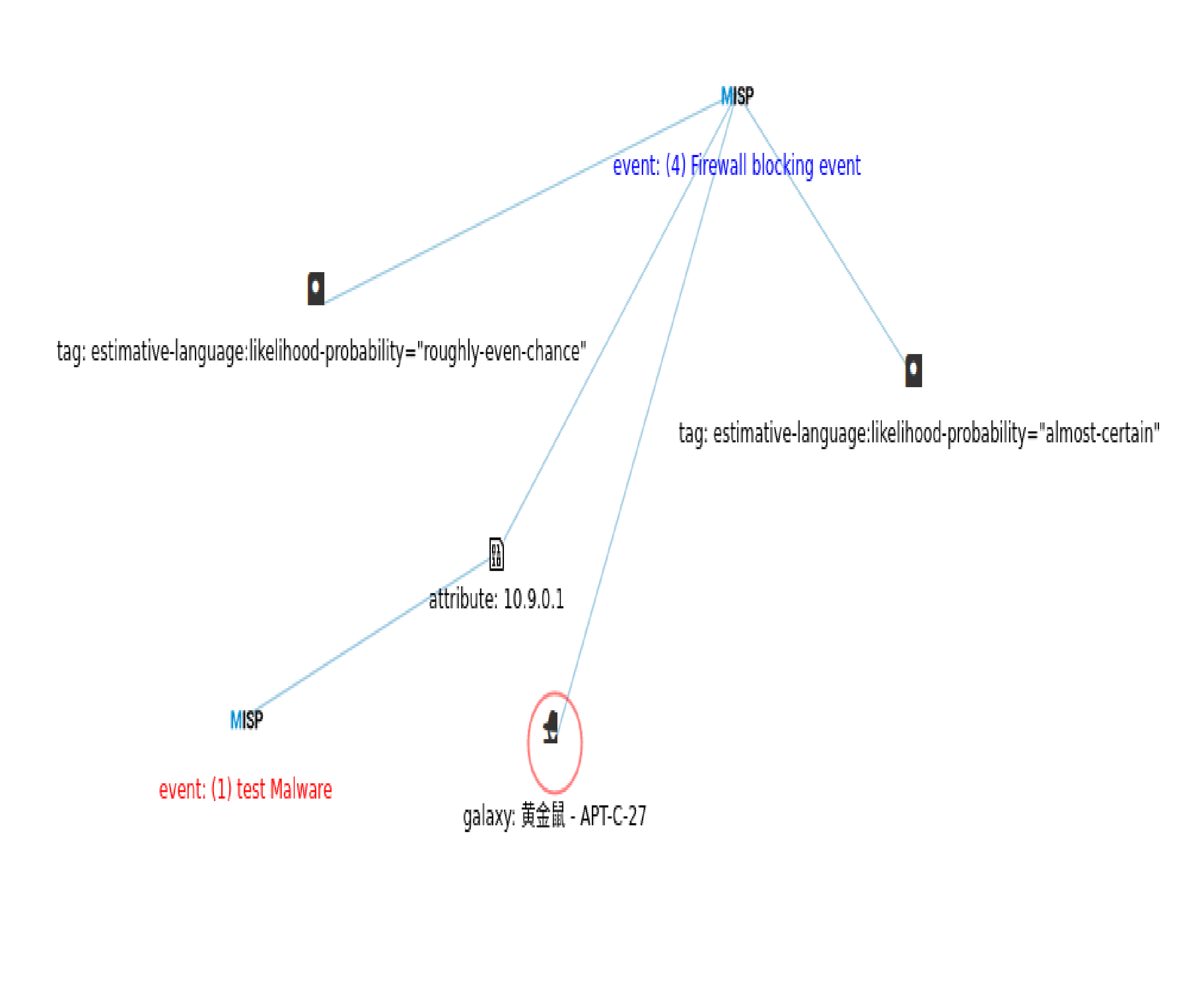
- **Data Modeling**: MISP uses a flexible data model that allows users to define and share threat intelligence information in a structured way. This includes information about malware, indicators of compromise (IoCs), attack techniques, and more.
- **Data Feeds**: Users can subscribe to various threat intelligence feeds and import data into MISP, enabling them to stay updated on the latest threats and vulnerabilities.
- **Sharing and Collaboration**: MISP facilitates the sharing of threat intelligence data between different organizations and sectors. Users can define access controls and sharing groups to control who has access to their data.
- **Integration**: MISP can be integrated with other security tools and platforms, allowing for automated data sharing and enrichment. This helps organizations streamline their threat intelligence processes.
- **Correlation and Analysis**: MISP provides features for correlating and analyzing threat data to identify patterns and potential threats. It supports the merging of data from different sources to create a more comprehensive picture of cyber threats.

Key Features

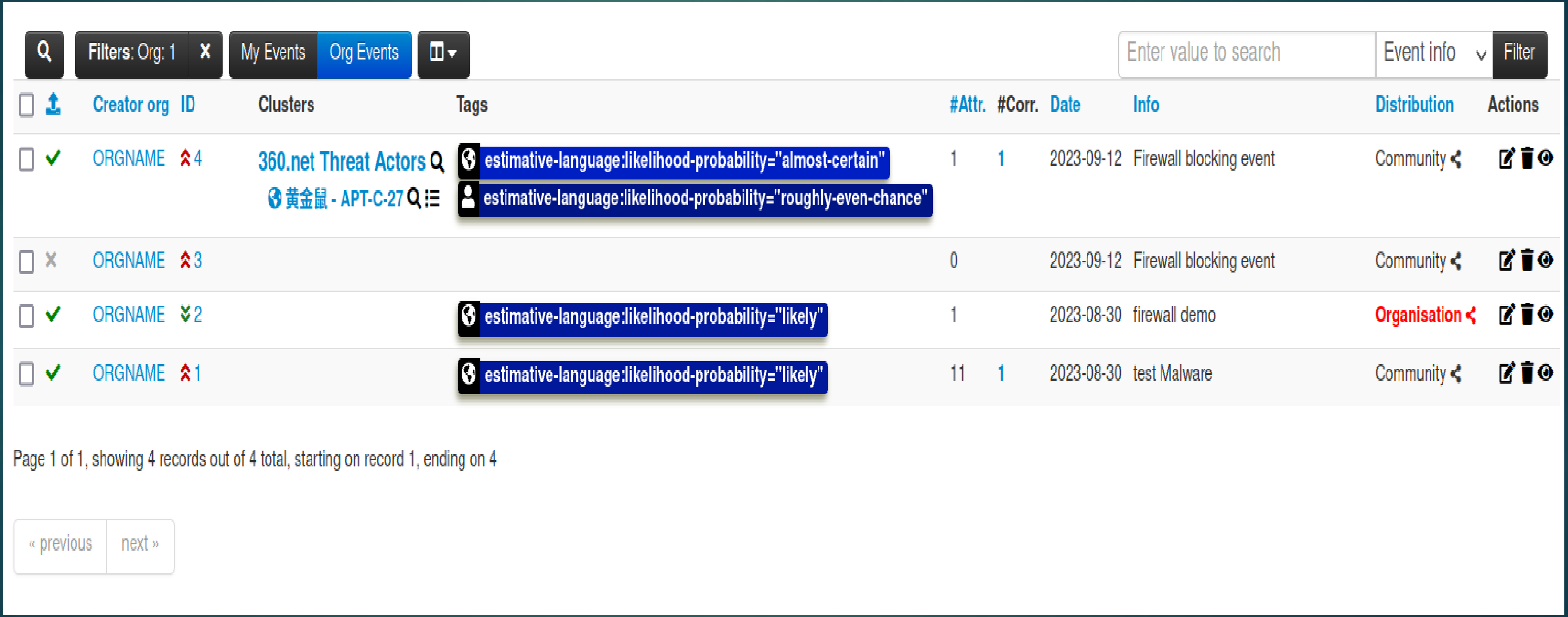
- **Stix/TAXII Support:** MISP uses the STIX (Structured Threat Information eXpression) and TAXII (Trusted Automated Exchange of Indicator Information) standards for representing and exchanging threat intelligence data.
- **Customization:** Users can customize MISP to fit their specific needs, including creating custom data models and adding extensions.
- **Community Support:** MISP has an active user community and is widely used in the cybersecurity community. Users can benefit from shared knowledge and best practices.
- **Security and Privacy:** MISP takes security and privacy seriously, allowing organizations to protect sensitive threat intelligence data and control access to it

Data modelling

1. **Attributes and Object Types**
2. **Event Structure**
3. **Data Sharing Formats**
4. **Customization**
5. **Data Validation**


MISP
event: (4) Firewall blocking event
tag: estimative-language:likelihood-probability="roughly-even-chance"
tag: estimative-language:likelihood-probability="almost-certain"
attribute: 10.9.0.1
MISP
event: (1) test Malware
galaxy: 黄金鼠 - APT-C-27

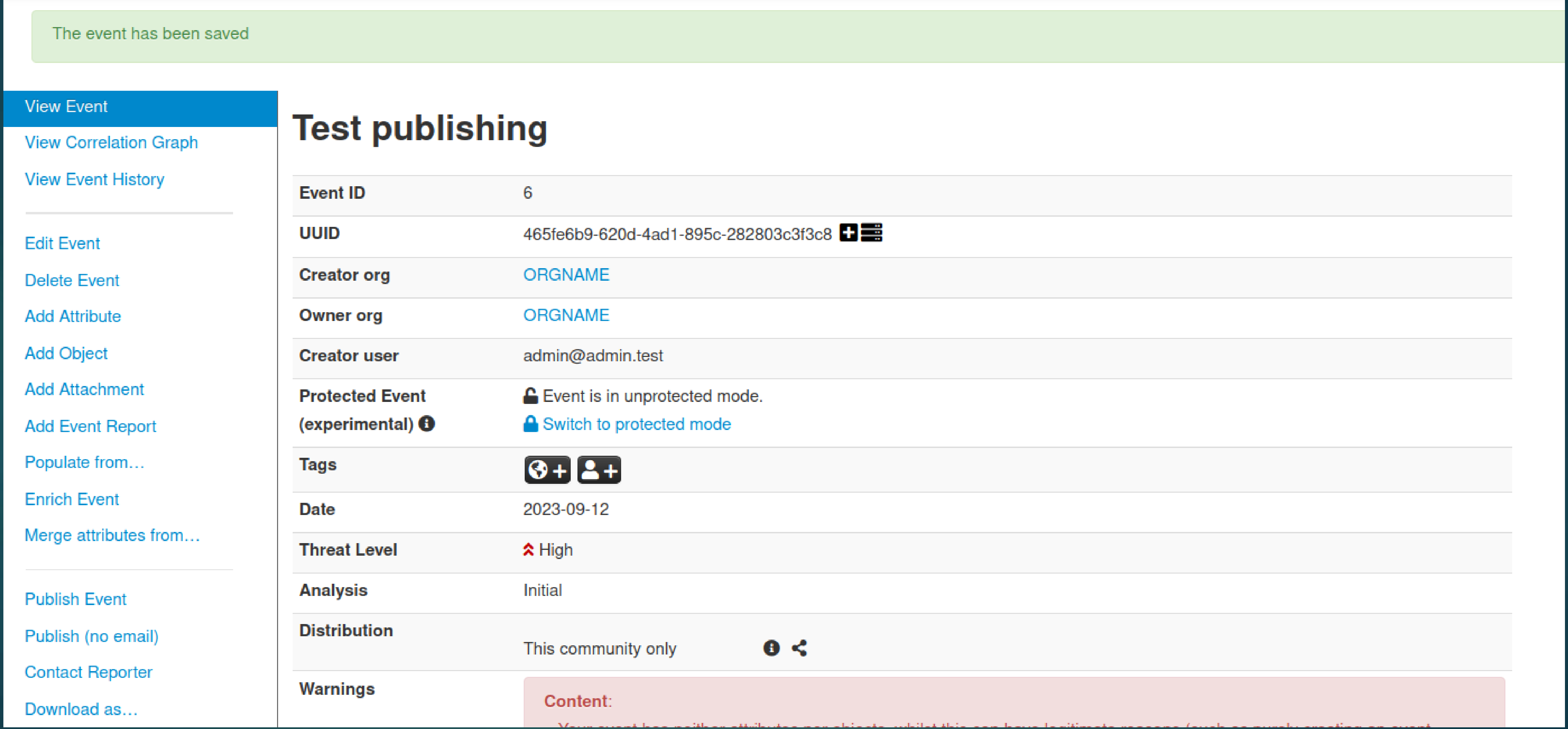
Data Feeds



☐		Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Info	Distribution	Actions
☐	✓	ORGNAME	4	360.net Threat Actors 黄金鼠 - APT-C-27	estimative-language:likelihood-probability="almost-certain" estimative-language:likelihood-probability="roughly-even-chance"	1	1	2023-09-12	Firewall blocking event	Community	
☐	✗	ORGNAME	3			0		2023-09-12	Firewall blocking event	Community	
☐	✓	ORGNAME	2		estimative-language:likelihood-probability="likely"	1		2023-08-30	firewall demo	Organisation	
☐	✓	ORGNAME	1		estimative-language:likelihood-probability="likely"	11	1	2023-08-30	test Malware	Community	

Page 1 of 1, showing 4 records out of 4 total, starting on record 1, ending on 4

Sharing and Collaboration



The event has been saved

- View Event
- View Correlation Graph
- View Event History
- Edit Event
- Delete Event
- Add Attribute
- Add Object
- Add Attachment
- Add Event Report
- Populate from…
- Enrich Event
- Merge attributes from…
- Publish Event
- Publish (no email)
- Contact Reporter
- Download as…

Test publishing

Event ID	6
UUID	465fe6b9-620d-4ad1-895c-282803c3f3c8
Creator org	ORGNAME
Owner org	ORGNAME
Creator user	admin@admin.test
Protected Event (experimental)	Event is in unprotected mode. Switch to protected mode
Tags	+ +
Date	2023-09-12
Threat Level	High
Analysis	Initial
Distribution	This community only
Warnings	Content:

- 1. Installation through Docker, Coolacid MISP : https://youtu.be/h_IxGcvjg8U
- Issue : Port must be changed in order to create MISP. After that, the password has to be changed with randomized long password. Password can be an issue if it is not given properly.