



## MISP-harjoitus

Juuso Leppänen, TTV22S3

Opiskelutehtävä

Kyberuhkatieto ja data-analytiikka TC6030-3011, Heikki Järvinen

8.12.2024

Tieto- ja viestintätekniikka

## Sisältö

<b>1</b>	<b>Johdanto .....</b>	<b>2</b>
<b>2</b>	<b>Mitä erilaisia jakeluasteita tapahtuman luomisessa voi käyttää? Mitä väliä jakeluasteella on? 2</b>	
2.1	Miksi jakeluasteella on väliä? .....	3
<b>3</b>	<b>Missä muodossa cybercrime-tracker.net toimittaa feedinsä? .....</b>	<b>3</b>
<b>4</b>	<b>Mikä käyttäjän "esko.morko" nids sid -numero on? .....</b>	<b>3</b>
<b>5</b>	<b>Kuinka monta attribuuttia löydät kyseisestä MISPistä aikaväliltä 1.9.2023-1.4.2024? ...</b>	<b>4</b>
<b>6</b>	<b>Minkä pankkiryhmän asiakas tapahtuman 1401 pahantekijä todennäköisesti on? .....</b>	<b>4</b>
<b>7</b>	<b>Kuinka monta virhettä varoitus- ja virhelokissa on? .....</b>	<b>5</b>
<b>8</b>	<b>Minkä niminen tagi on merkitty ID-numerolla 600?.....</b>	<b>5</b>
<b>9</b>	<b>Minkä nimiset aktiiviset tagit ovat taksonomikirjastossa honeypot-basic?.....</b>	<b>5</b>
<b>10</b>	<b>Mikä organisaatio on kaikista isoimmalla ID-numerolla järjestelmässä? .....</b>	<b>6</b>
<b>11</b>	<b>Mikä MISP-serveriasetus on kriittisesti vioittunut kyseisessä serverissä? .....</b>	<b>7</b>
	<b>Lähteet .....</b>	<b>9</b>
	<b>Liitteet .....</b>	<b>10</b>
	Liite 1. Liitteen otsikko .....	10
	Liite 2. Liitteen otsikko .....	11

## Kuviot

Kuvaotsikkoluettelon hakusanoja ei löytynyt.

## Taulukot

Kuvaotsikkoluettelon hakusanoja ei löytynyt.

Kuvaotsikkoluettelon hakusanoja ei löytynyt.

## 1 Johdanto

MISP (Malware Information Sharing Platform) on avoimen lähdekoodin työkalu, joka mahdollistaa kyberuhkien, kuten haittaohjelmien ja hyökkäysten, tiedon jakamisen organisaatioiden välillä. Tässä tehtävässä tutkitaan MISP-järjestelmän toimintoja, kuten jakeluasteita, attribuutteja ja ta-  
gien hallintaa, sekä analysoidaan järjestelmään liittyviä tietoja ja virheitä. Tarkoituksena on ymmärtää MISP:n käyttöä kyberuhkien havaitsemisessa ja hallinnassa.

## 2 Mitä erilaisia jakeluasteita tapahtuman luomisessa voi käyttää? Mitä väliä jakeluasteella on?

The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instance

[List Events](#)  
[Add Event](#)  
[Import from...](#)  
[REST client](#)  


---

[List Attributes](#)  
[Search Attributes](#)  


---

[View Proposals](#)  
[Events with proposals](#)  
[View delegation requests](#)  


---

[Export](#)  
[Automation](#)

### Add Event

Date

Threat Level ⓘ

Event Info

Extends Event

Distribution ⓘ  


Your organisation only  
This community only  
Connected communities  
All communities  
Sharing group

Your organization only: Tapahtuma jaetaan vain organisaatiolle, joka on luonut sen. Tämä rajoittaa tiedon jakamista muille organisaatioille.

This community only: Tapahtuma jaetaan vain tietyille yhteisöille, joihin organisaatio kuuluu. Tämä mahdollistaa tiedon jakamisen laajemmalle ryhmälle, mutta ei kaikille.

Connected communities: Tapahtuma jaetaan organisaation ja siihen liittyvien yhteisöjen jäsenille. Tämä jakeluaste laajentaa tiedon jakamista yhteisön muihin organisaatioihin, jotka ovat yhteydessä toisiinsa.

All communities: Tapahtuma jaetaan kaikille MISP-yhteisöille, jotka ovat mukana järjestelmässä. Tämä jakeluaste mahdollistaa tiedon leviämisen laajalle yleisölle, mikä voi edistää tiedon nopeaa levittämistä.

Sharing group: Tapahtuma jaetaan vain määritellyn jakeluryhmän jäsenille. Jakeluryhmä voi olla rajattu määrä organisaatioita tai käyttäjiä, jotka ovat osa erityistä yhteistyöryhmää.

## 2.1 Miksi jakeluasteella on väliä?

Jakeluasteella on merkittävä rooli tietoturvatiedon jakamisen hallinnassa ja turvallisuudessa. Se määrittelee, kuinka laajasti jaettu tieto päätyy organisaatioihin ja yhteisöihin, ja sen avulla voidaan kontrolloida, kuka saa pääsyn herkkään ja kriittiseen tietoon. Oikein asetettu jakeluaste auttaa suojaamaan luottamuksellista tietoa ja varmistamaan, että vain valtuutetut tahot saavat sen käyttöönsä.

## 3 Missä muodossa cybercrime-tracker.net toimittaa feedinsä?

Cybercrime-tracker.net toimittaa feedinsä muodossa freetext, eli vapaamuotoisena tekstinä.

## 4 Mikä käyttäjän "esko.morko" nids sid -numero on?

esko.morko nids sid numero on 5706234.

**Users index**

Click here to reset the API keys of all sync and org admin users in one shot. This will also automatically inform them of their new API keys.

« previous   next »

	ID	Org	Role	Email	Event alert	Contact alert	POP Key	NIDS SID	Terms Accepted	Last Login	Created	Disabled	Actions
<input type="checkbox"/>	95	Tammi-pankki	User	esko.morko@tammi.bank	x	x	x	5706234	x	2023-11-24 09:08:17	2023-11-24 08:36:43	x	<a href="#">edit</a> <a href="#">delete</a>

## 5 Kuinka monta attribuuttia löydät kyseisestä MISPistä aikaväliltä 1.9.2023-1.4.2024?

seuraavilla asetuksilla löytyi 54 attribuuttia.

[Home](#)
[Event Actions](#)
[Dashboard](#)
[Galaxies](#)
[Input Filters](#)
[Global Actions](#)
[Sync Actions](#)
[Administration](#)
[Logs](#)
[API](#)

[List Events](#)
[Add Event](#)
[Import from...](#)
[REST client](#)

[List Attributes](#)
[Search Attributes](#)

[View Proposals](#)
[Events with proposals](#)
[View delegation requests](#)

[Export](#)
[Automation](#)

### Search Attribute

You can search for attributes based on contained expression within the value, event ID, submitting organisation, category and type.

For the value, event ID and organisation, you can enter several search terms by entering each term as a new line. To exclude things from a result, use the NOT operator (!) in front of the term.

For string searches (such as searching for an expression, tags, etc) - lookups are simple string matches. If you want a substring match encapsulate the lookup string between "%" characters.

Containing the following expressions

Having tag or being an attribute of an event having the tag

Being attributes of the following event IDs, event UUIDs or attribute UUIDs

From the following organisation(s)

Type <sup>1</sup>  Category <sup>1</sup>

☐ Only find IOCs flagged as to IDS

#### First seen and Last seen

Attributes not having first seen or last seen set might not appear in the search

First seen date  Last seen date

First seen time  Last seen time

<sup>L</sup> Expected format: HH:MM:SS.ssssss+TT:TT <sup>L</sup> Expected format: HH:MM:SS.ssssss+TT:TT

## 6 Minkä pankkiryhmän asiakas tapahtuman 1401 pahantekijä todennäköi sesti on?

Tammi-pankki on todennäköisin vaihtoehto

Attributes													
Date	Event	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution
2023-10-02	1401	Tammi-pankki	Payload	delivery	sha256 b9c5d433809e0ad9a00443d4209f44b32319d54ab8480e9656081381c25			Ransomware Q Tamä sha-äro nähty ävstäässä sähkäläpostin metatietäjä.		273234 273182 160160 160065 165028 Q			Inherent event (beta)
2023-10-02	1401	Tammi-pankki	Financial	fraud	iban OKOYFHH123456781234567890			Pankkiklän numero, joka rahat piti laittaa.		Q			Your organisation only (beta)
2023-10-02	1401	Tammi-pankki	Payload	delivery	attachment iodeite.txt			Ransomware Q Ransomware Q		Q			Your organisation only (beta)
2023-10-02	1401	Tammi-pankki	Person	first-name	Paul			Ehänini löydety metatiedosta.		273236 Q			Inherent event (beta)
2023-10-02	1401	Tammi-pankki	Payload	delivery	filename Paulin_palka_tiedosto.txt			Tiedosta tiedoston nimi.		Q			Inherent event (beta)
2023-10-02	1401	Tammi-pankki	Payload	delivery	sha256 2ca2e55e0d3d74d9d903159023135d38da3630d0914e3d00b126335a58f0d			sha joka löytyi Paulin tiedostosta.		273180 160242 160063 165031 Q			Inherent event (beta)
2023-10-02	1401	Tammi-pankki	Network	activity	text https://www.viestiforumi.com/ga/46/12/82/828e000e4485708a322644c2351831a5f585a9802b2ca27e423d15f1b101de4e0c0f-624828e00e4485708a322644c2351831a5f585a9802b2ca27e423d15f1b101-149436619			Tiedot viestijorjunnasta.		Q			Inherent event (beta)

## 7 Kuinka monta virhettä varoitus- ja virhelokissa on?

0 kappaletta

Logs

< previous

next >

1 result

Authentication events

MSRP Update results

Testing changes

Warnings and errors

id 1

Email

Org

Created

Model

Model ID

Action

Title

Change

< previous

next >

**8 Minkä niminen tagi on merkitty ID-numerolla 600?**

Botnet "3101" on kyseinen tagi.

Tags										
<input type="text"/> Previous    Next <input type="button" value="+"/>										
Simple	Advanced									
ID	Exportable	Hidden	Local Only	Name	Restricted to org	Restricted to user	Taxonomy	Tagged events	Tagged attributes	Activity
500	✓	x	x	Student "1515"	x	x		1	0	✗
72	✓	x	x	StudentCourses.code="mastery"	x	x		0	0	✗

**9 Minkä nimiset aktiiviset tagit ovat taksonomiakirjastossa honeypot-basic?**

All		Enabled	Disabled	
ID ↑	Namespace	Description	Version	Enabled
105	osint	Open Source Intelligence - Classification (MISP taxonomies)	11	✗
79	infoleak	A taxonomy describing information leaks and especially information classified as being potentially leaked. The taxonomy is based on the work by CIRCL on the AIL framework. The taxonomy aim is to be used at large to improve classification of leaked information.	7	✗
72	honeypot-basic	Updated (CIRCL, Seamus Dowling and EURECOM) from Christian Seifert, Ian Welch, Peter Komarsarczuk, 'Taxonomy of Honeypots', Technical Report CS-TR-06/12, VICTORIA UNIVERSITY OF WELLINGTON, School of Mathematical and Computing Sciences, June 2006, <a href="http://www.mcs.vuw.ac.nz/comp/Publications/archive/CS-TR-06/CS-TR-06-12.pdf">http://www.mcs.vuw.ac.nz/comp/Publications/archive/CS-TR-06/CS-TR-06-12.pdf</a> .	4	✓

<

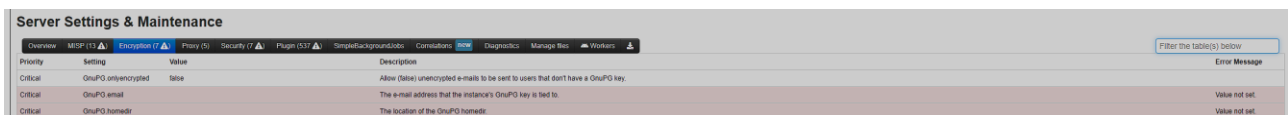
## 10 Mikä organisaatio on kaikista isoimmalla ID-numerolla järjestelmässä?

kaikista suurin organisaation ID-numero on 30, joka kuuluu organisaatio Pompadour:lle

Organisation Pompadour	
ID	30
UUID	edb265ec-c219-4f8f-b497-204e03d4cf9f
Local or remote	Local
Description	Kauneudenhoitotuoteliikeketju
Domain restrictions	pompadour.test
Created by	admin@admin.test
Creation time	2022-11-20 19:08:14
Last modified	2022-11-20 19:08:14
<a href="#">Members</a> <a href="#">Events</a> <a href="#">Sharing Groups</a>	

## 11 Mikä MISP-serveriasetus on kriittisesti vioittunut kyseisessä serverissä?

Tämä tehtävä osoittautui erittäin haastavaksi sillä en oikein tiennyt mitä olin etsimässä, mutta todennäköisin vaihtoehto voisi olla Redis salasanan puuttuminen. Liitän kuvat critical asioista mitä löysin.



The screenshot shows the 'Server Settings & Maintenance' page in the MISP interface. The 'Encryption' tab is active, showing a table of settings. Three settings are marked as 'Critical' and have error messages: 'GnuPG on/encrypted' is 'false', 'GnuPG email' is 'Value not set', and 'GnuPG homedir' is 'Value not set'.

Server Settings & Maintenance				
<a href="#">Overview</a> <a href="#">MISP (1)</a> <a href="#">Encryption (7)</a> <a href="#">Priority (5)</a> <a href="#">Security (7)</a> <a href="#">Plugins (3)</a> <a href="#">SimpleBackgroundJobs</a> <a href="#">Consistency</a> <a href="#">Diagnostics</a> <a href="#">Manage Res</a> <a href="#">Workers</a>				
Priority	Setting	Value	Description	Error Message
Critical	GnuPG on/encrypted	false	Allow (false) unencrypted e-mails to be sent to users that don't have a GnuPG key.	
Critical	GnuPG email		The e-mail address that the instance's GnuPG key is tied to.	Value not set.
Critical	GnuPG homedir		The location of the GnuPG homedir.	Value not set.



Priority	Setting	Value	Description	Error Message
Critical	MSPbaseurl	https://misp.bc502.via.5	The base url of the application (in the format https://www.mymispinstance.com or https://myserver.com/misp). Several features depend on this setting being correctly set to function.	The currently set baseurl does not match the URL through which you have accessed the page. Disregard this if you are accessing the page via an alternate URL (for example via IP address).
Critical	MSPexternal_baseurl		The base url of the application (in the format https://www.mymispinstance.com) as visible externally by other MSPs. MSP will encode this URL in sharing groups when including itself. If this value is not set, the baseurl is used as a fallback.	Value not set.
Critical	MSPlive	true	Unless set to true, the instance will only be accessible by site admins.	
Critical	MSPlanguage	eng	Select the language MSP should use. The default is english.	
Critical	MSPcorrelation_engine		Choose which correlation engine to use. MSP defaults to the default engine, maintaining all data in the database whilst enforcing ACL rules on any non site-admin user. This is recommended for any MSP instance with multiple organisations. If you are an endpoint MSP, consider switching to the much leaner and faster No ACL engine.	
Critical	MSPcorrelation_limit	100	Set a value for the maximum number of correlations a value should have before MSP will refuse to correlate it (extremely over-correlating values are rarely useful from a correlation perspective).	
Critical	MSPenable_advanced_correlations	false	Enable some performance heavy correlations (currently CDR correlation)	
Critical	MSPhost_pg_id	adminorg	The hosting organisation of this instance. If this is not selected then replication instances cannot be added.	
Critical	MSPuuid	e2396b6-51a5-4702-a869-58649d9af93	The MSP instance UUID. This UUID is used to identify this instance.	No valid UUID set
Critical	MSPshoworg	true	Setting this setting to 'false' will hide all organisation names / logos.	
Critical	MSPouser	www-data	The Unix user MSP (php) is running as	
Critical	MSPemail	email@example.com	The e-mail address that MSP should use for all notifications	
Critical	MSPdisable_emailing	false	You can disable all e-mailing using this setting. When enabled, no outgoing e-mails will be sent by MSP.	
Critical	MSPdefault_event_distribution	This community only	The default distribution setting for events (0-3).	
Critical	MSPdefault_attribute_distribution	Inherit from event	The default distribution setting for attributes, set it to 'event' if you would like the attributes to default to the event distribution level (0-3 or 'event')	
Critical	MSPdefault_event_tag_collection	None	The tag collection to be applied to all events created manually.	
Critical	MSPdefault_publish_alert	true	The default setting for publish alerts when creating users.	
Critical	MSPdisable_taxonomy_consistency_checks	false	*WARNING* This will disable taxonomy tags conflict checks when browsing attributes and objects, does not impact checks when adding tags. It can dramatically increase the performance when loading events with lots of tagged attributes or objects.	
Critical	MSPlog_skip_db_logs_completely	false	This functionality allows you to completely disable any logs from being saved in your SQL backend. This is HIGHLY advised against, you lose all the functionalities provided by the audit log subsystem along with the event history (as these are built based on the logs on the fly). Only enable this if you understand and accept the associated risks.	Logging has now been disabled - your audit logs will not capture failed authentication attempts, your event history logs are not being populated and no system maintenance messages are being logged.
Critical	MSPlog_paramod	false	If this functionality is enabled all page requests will be logged. Keep in mind this is extremely verbose and will become a burden to your database.	
Critical	MSPlog_paramod_skip_db	false	You can decide to skip the logging of the paramod logs to the database.	
Critical	MSPlog_paramod_include_post_body	false	If paramod logging is enabled, include the POST body in the entries.	
Critical	MSPlog_user_ips	false	Log user IPs on each request. 30 day retention for lookups by IP to get the last authenticated user ID for the given IP, whilst on the reverse, indefinitely stores all associated IPs for a user ID.	
Critical	MSPpropagate_block_attributes	false	Enable this setting to allow blocking attributes from to_ids sensitive exports if a proposal has been made to it to remove the IDS flag or to remove the attribute altogether. This is a powerful tool to deal with false-positives efficiently.	
Critical	MSPcompletely_disable_correlation	false	*WARNING* This setting will completely disable the correlation on this instance and remove any existing saved correlations. Enabling this will trigger a full recorelation of all data which is an extremely long and costly procedure. Only enable this if you know what you're doing.	
Critical	MSPallow_disabling_correlation	false	*WARNING* This setting will give event creators the possibility to disable the correlation of individual events / attributes that they have created.	
Critical	MSPredis_host	redis	The host running the redis server to be used for generic MSP tasks such as caching. This is not to be confused by the redis server used by the background processing.	
Critical	MSPredis_port	6379	The port used by the redis server to be used for generic MSP tasks such as caching. This is not to be confused by the redis server used by the background processing.	
Critical	MSPredis_database	13	The database on the redis server to be used for generic MSP tasks. If you run more than one MSP instance, please make sure to use a different database on each instance.	
Critical	MSPredis_password	****	The password on the redis server (if any) to be used for generic MSP tasks.	

Priority	Setting	Value	Description	Error Message
Critical	MSPbaseurl	https://misp.bc502.via.5	The base url of the application (in the format https://www.mymispinstance.com or https://myserver.com/misp). Several features depend on this setting being correctly set to function.	The currently set baseurl does not match the URL through which you have accessed the page. Disregard this if you are accessing the page via an alternate URL (for example via IP address).
Critical	MSPexternal_baseurl		The base url of the application (in the format https://www.mymispinstance.com) as visible externally by other MSPs. MSP will encode this URL in sharing groups when including itself. If this value is not set, the baseurl is used as a fallback.	Value not set.
Critical	MSPlive	true	Unless set to true, the instance will only be accessible by site admins.	
Critical	MSPlanguage	eng	Select the language MSP should use. The default is english.	
Critical	MSPcorrelation_engine		Choose which correlation engine to use. MSP defaults to the default engine, maintaining all data in the database whilst enforcing ACL rules on any non site-admin user. This is recommended for any MSP instance with multiple organisations. If you are an endpoint MSP, consider switching to the much leaner and faster No ACL engine.	
Critical	MSPcorrelation_limit	100	Set a value for the maximum number of correlations a value should have before MSP will refuse to correlate it (extremely over-correlating values are rarely useful from a correlation perspective).	
Critical	MSPenable_advanced_correlations	false	Enable some performance heavy correlations (currently CDR correlation)	
Critical	MSPhost_pg_id	adminorg	The hosting organisation of this instance. If this is not selected then replication instances cannot be added.	
Critical	MSPuuid	e2396b6-51a5-4702-a869-58649d9af93	The MSP instance UUID. This UUID is used to identify this instance.	No valid UUID set
Critical	MSPshoworg	true	Setting this setting to 'false' will hide all organisation names / logos.	
Critical	MSPouser	www-data	The Unix user MSP (php) is running as	
Critical	MSPemail	email@example.com	The e-mail address that MSP should use for all notifications	
Critical	MSPdisable_emailing	false	You can disable all e-mailing using this setting. When enabled, no outgoing e-mails will be sent by MSP.	
Critical	MSPdefault_event_distribution	This community only	The default distribution setting for events (0-3).	
Critical	MSPdefault_attribute_distribution	Inherit from event	The default distribution setting for attributes, set it to 'event' if you would like the attributes to default to the event distribution level (0-3 or 'event')	
Critical	MSPdefault_event_tag_collection	None	The tag collection to be applied to all events created manually.	
Critical	MSPdefault_publish_alert	true	The default setting for publish alerts when creating users.	
Critical	MSPdisable_taxonomy_consistency_checks	false	*WARNING* This will disable taxonomy tags conflict checks when browsing attributes and objects, does not impact checks when adding tags. It can dramatically increase the performance when loading events with lots of tagged attributes or objects.	
Critical	MSPlog_skip_db_logs_completely	false	This functionality allows you to completely disable any logs from being saved in your SQL backend. This is HIGHLY advised against, you lose all the functionalities provided by the audit log subsystem along with the event history (as these are built based on the logs on the fly). Only enable this if you understand and accept the associated risks.	Logging has now been disabled - your audit logs will not capture failed authentication attempts, your event history logs are not being populated and no system maintenance messages are being logged.
Critical	MSPlog_paramod	false	If this functionality is enabled all page requests will be logged. Keep in mind this is extremely verbose and will become a burden to your database.	
Critical	MSPlog_paramod_skip_db	false	You can decide to skip the logging of the paramod logs to the database.	
Critical	MSPlog_paramod_include_post_body	false	If paramod logging is enabled, include the POST body in the entries.	
Critical	MSPlog_user_ips	false	Log user IPs on each request. 30 day retention for lookups by IP to get the last authenticated user ID for the given IP, whilst on the reverse, indefinitely stores all associated IPs for a user ID.	
Critical	MSPpropagate_block_attributes	false	Enable this setting to allow blocking attributes from to_ids sensitive exports if a proposal has been made to it to remove the IDS flag or to remove the attribute altogether. This is a powerful tool to deal with false-positives efficiently.	
Critical	MSPcompletely_disable_correlation	false	*WARNING* This setting will completely disable the correlation on this instance and remove any existing saved correlations. Enabling this will trigger a full recorelation of all data which is an extremely long and costly procedure. Only enable this if you know what you're doing.	
Critical	MSPallow_disabling_correlation	false	*WARNING* This setting will give event creators the possibility to disable the correlation of individual events / attributes that they have created.	
Critical	MSPredis_host	redis	The host running the redis server to be used for generic MSP tasks such as caching. This is not to be confused by the redis server used by the background processing.	
Critical	MSPredis_port	6379	The port used by the redis server to be used for generic MSP tasks such as caching. This is not to be confused by the redis server used by the background processing.	
Critical	MSPredis_database	13	The database on the redis server to be used for generic MSP tasks. If you run more than one MSP instance, please make sure to use a different database on each instance.	
Critical	MSPredis_password	****	The password on the redis server (if any) to be used for generic MSP tasks.	

## Lähteet

Kirjoita tähän lähdeluettelo.

## **Liitteet**

### **Liite 1. Liitteen otsikko**

**Liite 2. Liitteen otsikko**