



## MISP-harjoitus

Juuso Leppänen, TTV22S3

Opiskelutehtävä  
Kyberuhkatieto ja data-analytiikka TC6030-3011, Heikki Järvinen  
8.12.2024  
Tieto- ja viestintätteknikka

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

## Kuviot

Kuvaotsikkoluetteloon hakusanoja ei löytynyt.

## Taulukot

Kuvaotsikkoluetteloon hakusanoja ei löytynyt.

Kuvaotsikkoluetteloon 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 tien hallintaa, sekä analysoidaan järjestelmään liittyviä tietoja ja virheitä. Tarkoituksesta 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		
Add Event	Date	Distribution <small>i</small>	
Import from...	2024-12-07	This community only	
REST client	Threat Level <small>i</small> High		
List Attributes	Event Info Quick Event Description or Tracking		
Search Attributes	Extends Event Event UUID or ID. Leave blank if not applicable.		
View Proposals			
Events with proposals			
View delegation requests			
Export			
Automation	Submit		

The screenshot shows the 'Add Event' form in the MISP interface. On the left is a sidebar with links like 'List Events', 'Add Event' (which is selected and highlighted in blue), 'Import from...', 'REST client', etc. The main area has fields for 'Date' (set to 2024-12-07), 'Threat Level' (set to 'High'), 'Event Info' (containing 'Quick Event Description or Tracking'), and an 'Extends Event' field (containing 'Event UUID or ID. Leave blank if not applicable.'). A prominent feature is the 'Distribution' dropdown menu, which is open and shows five options: 'Your organisation only', 'This community only' (which is highlighted in dark grey), 'Connected communities', 'All communities', and 'Sharing group'. The 'This community only' option is currently selected.

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 levämisen 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 käytönsä.

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

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

seuraavilla asetuksilla löytyi 54 attribuutta.

The screenshot shows the MISP search interface with the following search parameters:

- Containing the following expressions:** An empty text input field.
- Having tag or being an attribute of an event having the tag:** An empty text input field.
- Being attributes of the following event IDs, event UUIDs or attribute UUIDs:** An empty text input field.
- From the following organisation(s):** An empty text input field.
- Type:** ALL
- Category:** ALL
- Only find IOCs flagged as to IDS**: Unchecked checkbox
- First seen and Last seen:**
  - First seen date:** 2023-09-01
  - Last seen date:** 2024-04-01
  - First seen time:** HH:MM:SS.ssssss+TT:TT
  - Last seen time:** HH:MM:SS.ssssss+TT:TT
- Search:** Button

## 6 Minkä pankkiryhmin 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
2023-19-02	1401 Tammi-pankki	Payload delivery	sha256	bd5d433989ed9e0044d3d20944a32819a54abf840b9e650d1391c25				Ransomware Q WannaCry Q	Tämä shie-avio nähti avattessa sähköpostin metalliseja.	27224 273182 166160 156085 165938 Q
2023-19-02	1401 Tammi-pankki	Financial fraud	iban	OKYOFIHH123456781234567890				Pankkitilin numero, jolle rahat piti taitaa		
2023-19-02	1401 Tammi-pankki	Payload delivery	attachment	tosite.txt				Ransomware Q WannaCry Q		
2023-19-02	1401 Tammi-pankki	Person	first-name	Paul				Elutimi lyödetti mettäleissä.	272238 Q	
2023-19-02	1401 Tammi-pankki	Payload delivery	filename	Paulin_paha_tiedosto.txt				Tiedossä tiedoston nimi.		
2023-19-02	1401 Tammi-pankki	Payload delivery	sha256	2ca26559e03d74de0da3156023135b39da3630cb914a3600b1263356c590d				sha (joka siity) Paulin_tiedosto	273180 156242 166063 155937 Q	
2023-19-02	1401 Tammi-pankki	Network activity	text	https://www.virustotal.com/file/f2d2d2be000e44fb70a32264422351611afbb8a982b2ce27e423dc1cf1fb1/detection%				Tiedot virustunnisteesta		

Page 1 of 1, showing 7 records out of 7 total, starting on record 1, ending on 7

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

0 kappaletta

Logs								
« previous	next »							
<a href="#">Email</a>	<a href="#">Authentication issues</a>	<a href="#">MISP Update results</a>	<a href="#">Setting changes</a>	<a href="#">Warnings and errors</a>				
« previous	next »							

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

Botnet "3101" on kyseinen tagi.

Tags									
ID	Exportable	Hidden	Local Only	Name	Restricted to org	Restricted to user	Taxonomy	Tagged events	Tagged attributes
600	✓	✗	✗	Botnet "3101"	✗	✗		1	0
72	✓	✗	✗	scam/malicious code - "malware"	✗	✗		9	0

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

All	Enabled	Disabled	Description	Version	Enabled
ID	Namespace				
105	oint		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 CIRO on the OIL 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 Komisarczuk, 'Taxonomy of Honeybots', 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	✓

HONEYBOT-BASIC Taxonomy Library										
ID	Namespace	Description	Version	Enabled	Action					
105	oint	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 CIRO on the OIL 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 Komisarczuk, 'Taxonomy of Honeybots', 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	✓						
Taxonomy Tags										
« previous	next »									
All	Enabled	Disabled	Name	Numerical Value	# Events	# Attributes	Tag	Enabled	Actions	
			honeypot-basic:communication-interface-'hardware-interface'	0	0	0	honeypot.basic:communication-interface-'hardware-interface'	✓	✖️	
			honeypot-basic:communication-interface-'network-interface'	0	0	0	honeypot.basic:communication-interface-'network-interface'	✓	✖️	
			honeypot-basic:communication-interface-'software-api'	0	0	0	honeypot.basic:communication-interface-'software-api'	✓	✖️	
			honeypot-basic:containment-'block'	1	0	0	honeypot.basic:containment-'block'	✓	✖️	
			honeypot-basic:containment-'defuse'	0	0	0	honeypot.basic:containment-'defuse'	✓	✖️	
			honeypot-basic:containment-'none'	0	0	0	honeypot.basic:containment-'none'	✓	✖️	
			honeypot-basic:containment-'slow-down'	0	0	0	honeypot.basic:containment-'slow-down'	✓	✖️	
			honeypot-basic:data-capture-'attack'	1	0	0	honeypot.basic:data-capture-'attack'	✓	✖️	
			honeypot-basic:data-capture-'events'	0	0	0	honeypot.basic:data-capture-'events'	✓	✖️	
			honeypot-basic:data-capture-'intrusions'	0	0	0	honeypot.basic:data-capture-'intrusions'	✓	✖️	
			honeypot-basic:data-capture-'network-capture'	0	0	0	honeypot.basic:data-capture-'network capture'	✓	✖️	
			honeypot-basic:data-capture-'none'	0	0	0	honeypot.basic:data-capture-'none'	✓	✖️	
			honeypot-basic:distribution-appearance-'distributed'	0	0	0	honeypot.basic:distribution-appearance-'distributed'	✓	✖️	
			honeypot-basic:distribution-appearance-'stand-alone'	0	0	0	honeypot.basic:distribution-appearance-'stand alone'	✓	✖️	
			honeypot-basic:interaction-level-'adaptive'	0	0	0	honeypot.basic:interaction-level-'adaptive'	✓	✖️	
			honeypot-basic:interaction-level-'high'	0	0	0	honeypot.basic:interaction-level-'high'	✓	✖️	
			honeypot-basic:interaction-level-'low'	0	0	0	honeypot.basic:interaction-level-'low'	✓	✖️	
			honeypot-basic:interaction-level-'medium'	0	0	0	honeypot.basic:interaction-level-'medium'	✓	✖️	
			honeypot-basic:interaction-level-'none'	0	0	0	honeypot.basic:interaction-level-'none'	✓	✖️	
			honeypot-basic:role-'client'	0	0	0	honeypot.basic:role-'client'	✓	✖️	
			honeypot-basic:role-'server'	0	0	0	honeypot.basic:role-'server'	✓	✖️	

Page 1 of 1, showing 1 records out of 21 total, starting on record 1, ending on 21

« previous next »

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

kaikista suurin organisaation ID-numero on 30, joka kuuluu organisaatio Pompadourille

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.

Server Settings & Maintenance			
Priority	Setting	Value	Description
Critical	OnuPO.onUnencrypted	false	Allow (false) unencrypted e-mails to be sent to users that don't have a OnuPO key.
Critical	OnuPO.email		The e-mail address that the instance's OnuPO key is tied to.
Critical	OnuPO.homeDir		The location of the OnuPO homedir.

Priority	Setting	Value	Description	Error Message
Critical	MISP_baseurl	https://misp.t0c60z.vie.5	The base url of the application (in the format https://www.myspinstance.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	MISP_external_baseurl		The base url of the application (in the format https://www.myspinstance.com) as visible externally by other MISP's. MISP 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	MISP_live	true	Unless set to true, the instance will only be accessible by site admins.	
Critical	MISP_language	eng	Select the language MISP should use. The default is english.	
Critical	MISP_correlation_engine		Choose which correlation engine to use. MISP 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 MISP instance with multiple organisations. If you are an endpoint MISP, consider switching to the much leaner and faster No ACL engine.	
Critical	MISP.correlation_limit	100	Set a value for the maximum number of correlations a value should have before MISP will refuse to correlate it (extremely over-correlating values are rarely useful from a correlation perspective).	
Critical	MISP.enable_advanced_correlations	false	Enable some performance heavy correlations (currently CIDR correlation)	
Critical	MISP.host.org_id	adminorg	The hosting organisation of this instance. If this is not selected then replication instances cannot be added.	
Critical	MISP.uuid	e239f686-51a5-4702-a869-56549daff93	The MISP instance UUID. This UUID is used to identify this instance.	No valid UUID set
Critical	MISP.showorg	true	Setting this setting to 'false' will hide all organisation names / logos.	
Critical	MISP.osuser	www-data	The Unix user MISP (php) is running as	
Critical	MISP_email	email@example.com	The e-mail address that MISP should use for all notifications	
Critical	MISP_disable_emailing	false	You can disable all e-mailing using this setting. When enabled, no outgoing e-mails will be sent by MISP.	
Critical	MISP.default_event_distribution	This community only	The default distribution setting for events (0-3).	
Critical	MISP.default_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	MISP.default_event_tag_collection	None	The tag collection to be applied to all events created manually.	
Critical	MISP.default_public_alert	true	The default setting for public alerts when creating users.	
Critical	MISP.disable_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	MISP_log_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	MISP.log_paranoia	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	MISP_log_paranoia_skip_db	false	You can decide to skip the logging of the paranoid logs to the database.	
Critical	MISP_log_paranoia_include_post_body	false	If paranoid logging is enabled, include the POST body in the entries.	
Critical	MISP_log_user_ip	false	Log user IPs on each request. 30 day retention for logups 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	MISPproposals_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	MISP_completely_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 re-correlation of all data which is an extremely long and costly procedure. Only enable this if you know what you're doing.	
Critical	MISP_allow_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	MISP.redis_host	redis	The host running the redis server to be used for generic MISP tasks such as caching. This is not to be confused by the redis server used by the background processing.	
Critical	MISP.redis_port	6379	The port used by the redis server to be used for generic MISP tasks such as caching. This is not to be confused by the redis server used by the background processing.	
Critical	MISP.redis_database	13	The database on the redis server to be used for generic MISP tasks. If you run more than one MISP instance, please make sure to use a different database on each instance.	
Critical	MISP.redis_password	*****	The password on the redis server (if any) to be used for generic MISP tasks.	

Priority	Setting	Value	Description	Error Message
Critical	MISP_baseurl	https://misp.t0c60z.vie.5	The base url of the application (in the format https://www.myspinstance.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	MISP_external_baseurl		The base url of the application (in the format https://www.myspinstance.com) as visible externally by other MISP's. MISP 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	MISP_live	true	Unless set to true, the instance will only be accessible by site admins.	
Critical	MISP_language	eng	Select the language MISP should use. The default is english.	
Critical	MISP.correlation_engine		Choose which correlation engine to use. MISP 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 MISP instance with multiple organisations. If you are an endpoint MISP, consider switching to the much leaner and faster No ACL engine.	
Critical	MISP.correlation_limit	100	Set a value for the maximum number of correlations a value should have before MISP will refuse to correlate it (extremely over-correlating values are rarely useful from a correlation perspective).	
Critical	MISP.enable_advanced_correlations	false	Enable some performance heavy correlations (currently CIDR correlation)	
Critical	MISP.host.org_id	adminorg	The hosting organisation of this instance. If this is not selected then replication instances cannot be added.	
Critical	MISP.uuid	e239f686-51a5-4702-a869-56549daff93	The MISP instance UUID. This UUID is used to identify this instance.	No valid UUID set
Critical	MISP.showorg	true	Setting this setting to 'false' will hide all organisation names / logos.	
Critical	MISP.osuser	www-data	The Unix user MISP (php) is running as	
Critical	MISP_email	email@example.com	The e-mail address that MISP should use for all notifications	
Critical	MISP_disable_emailing	false	You can disable all e-mailing using this setting. When enabled, no outgoing e-mails will be sent by MISP.	
Critical	MISP.default_event_distribution	This community only	The default distribution setting for events (0-3).	
Critical	MISP.default_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	MISP.default_event_tag_collection	None	The tag collection to be applied to all events created manually.	
Critical	MISP.default_public_alert	true	The default setting for public alerts when creating users.	
Critical	MISP.disable_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	MISP_log_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	MISP_log_paranoia	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	MISP_log_paranoia_skip_db	false	You can decide to skip the logging of the paranoid logs to the database.	
Critical	MISP_log_paranoia_include_post_body	false	If paranoid logging is enabled, include the POST body in the entries.	
Critical	MISP_log_user_ip	false	Log user IPs on each request. 30 day retention for logups 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	MISPproposals_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	MISP_completely_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 re-correlation of all data which is an extremely long and costly procedure. Only enable this if you know what you're doing.	
Critical	MISP_allow_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	MISP.redis_host	redis	The host running the redis server to be used for generic MISP tasks such as caching. This is not to be confused by the redis server used by the background processing.	
Critical	MISP.redis_port	6379	The port used by the redis server to be used for generic MISP tasks such as caching. This is not to be confused by the redis server used by the background processing.	
Critical	MISP.redis_database	13	The database on the redis server to be used for generic MISP tasks. If you run more than one MISP instance, please make sure to use a different database on each instance.	
Critical	MISP.redis_password	*****	The password on the redis server (if any) to be used for generic MISP tasks.	

## Lähteet

Kirjoita täähän lähdeluettelo.

## **Liitteet**

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

**Liite 2. Liitteen otsikko**