MISP-harjoitus

Juuso Leppänen, TTV22S3

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

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

Sisältö

Kuviot

Kuvaotsikkoluettelon hakusanoja ei löytynyt.

Taulukot

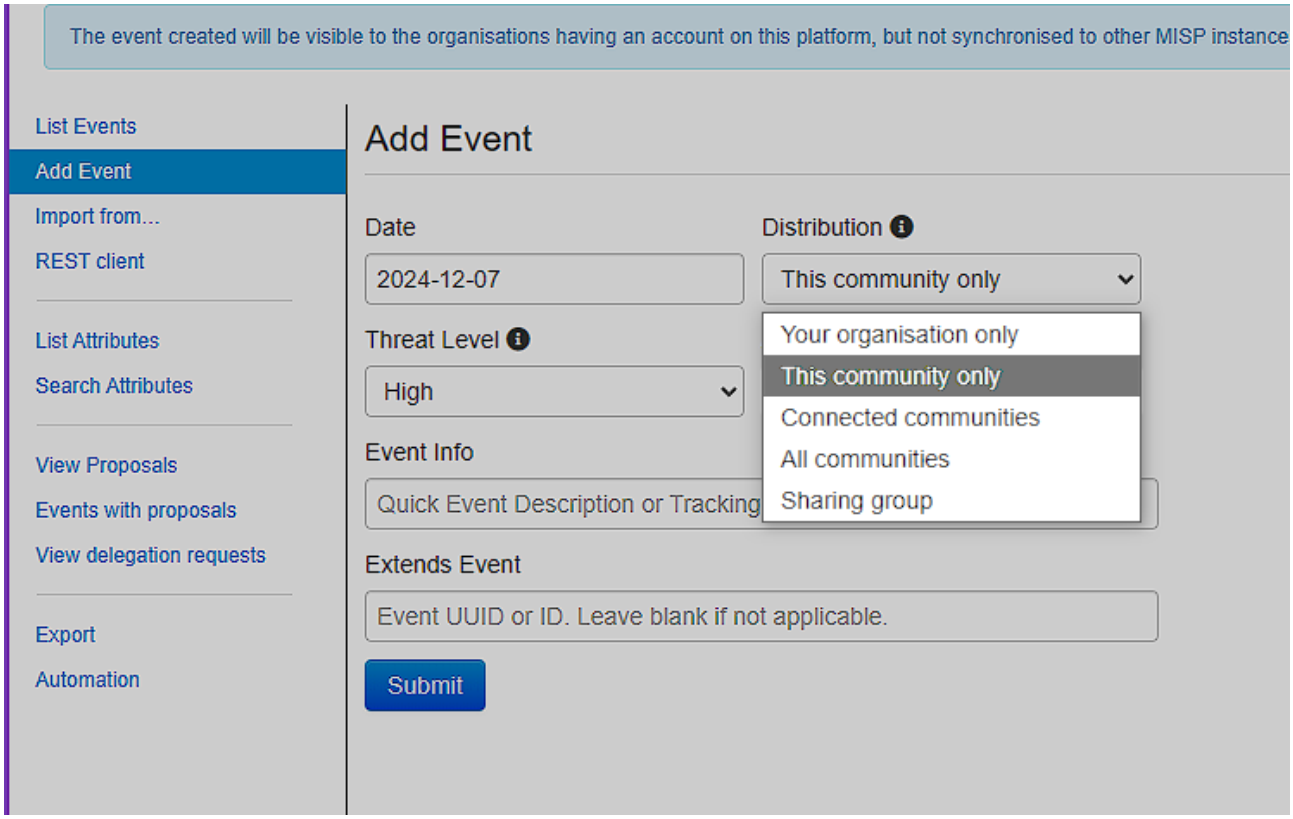
Kuvaotsikkoluettelon hakusanoja ei löytynyt.

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 tagien 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?



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?

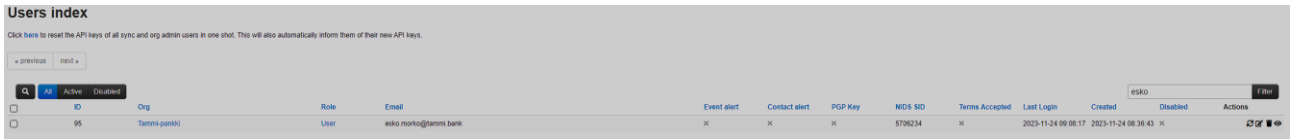
Jakeluasteella on merkittävä rooli tietoturvatiedon jakamisen hallinnassa ja turvallisuudessa. Se määrittelee, kuinka laajasti jaettu tieto päätyy organisaatioihin ja yhteisöihin, ja sen avulla voidaan kontrolloida, kuka saa pääsyn herkkään ja kriittiseen tietoon. Oikein asetettu jakeluaste auttaa suojaamaan 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.

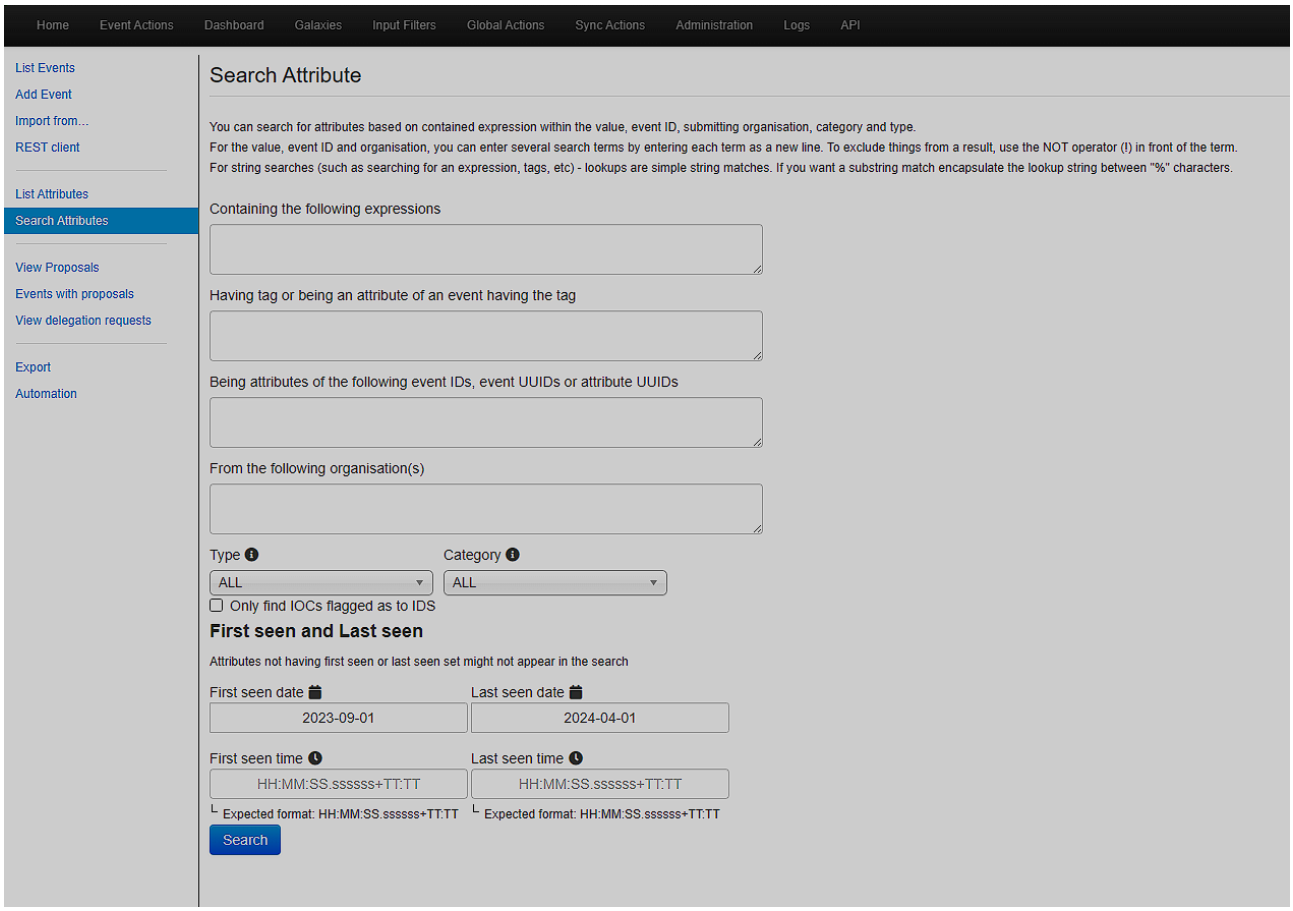
4 Mikä käyttäjän "esko.morko" nids sid -numero on?

esko.morko nids sid numero on 5706234.



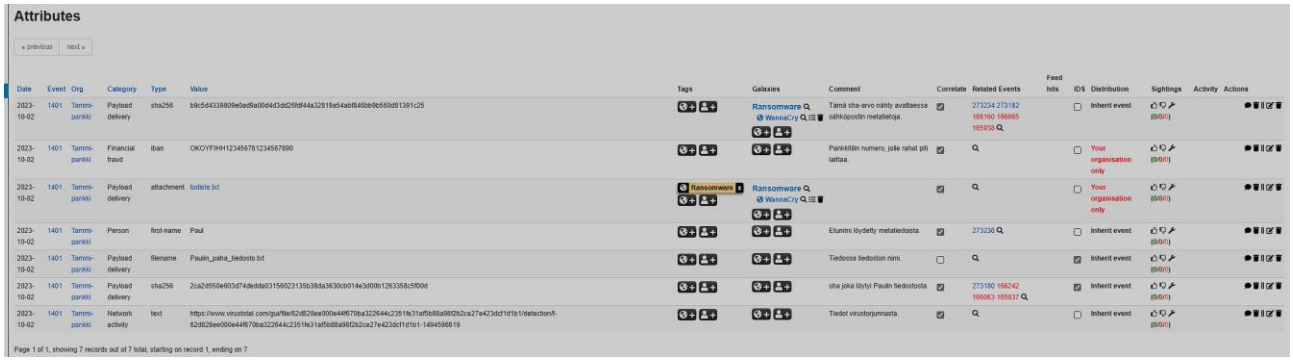
5 Kuinka monta attribuuttia löydät kyseisestä MISPistä aikaväliltä 1.9.2023-1.4.2024?

seuraavilla asetuksilla löytyi 54 attribuuttia.



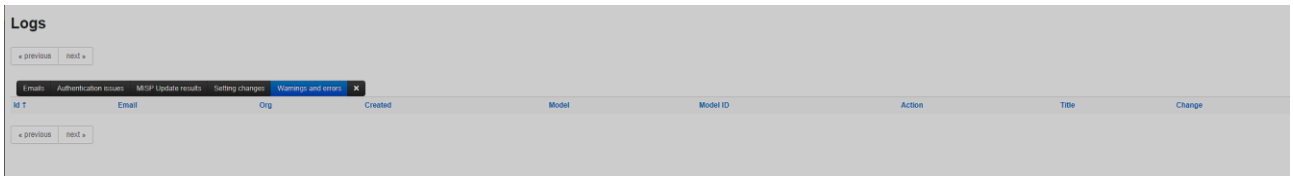
6 Minkä pankkiryhmän asiakas tapahtuman 1401 pahantekijä todennäköi sesti on?

Tammi-pankki on todennäköisin vaihtoehto



7 Kuinka monta virhettä varoitus- ja virhelokissa on?

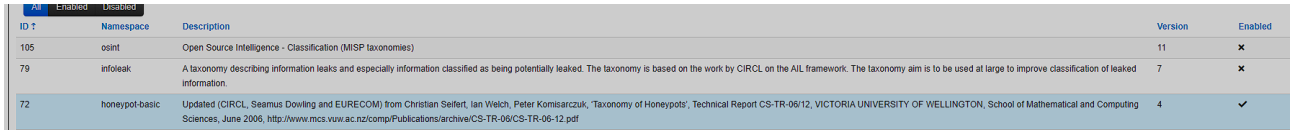
0 kappaletta

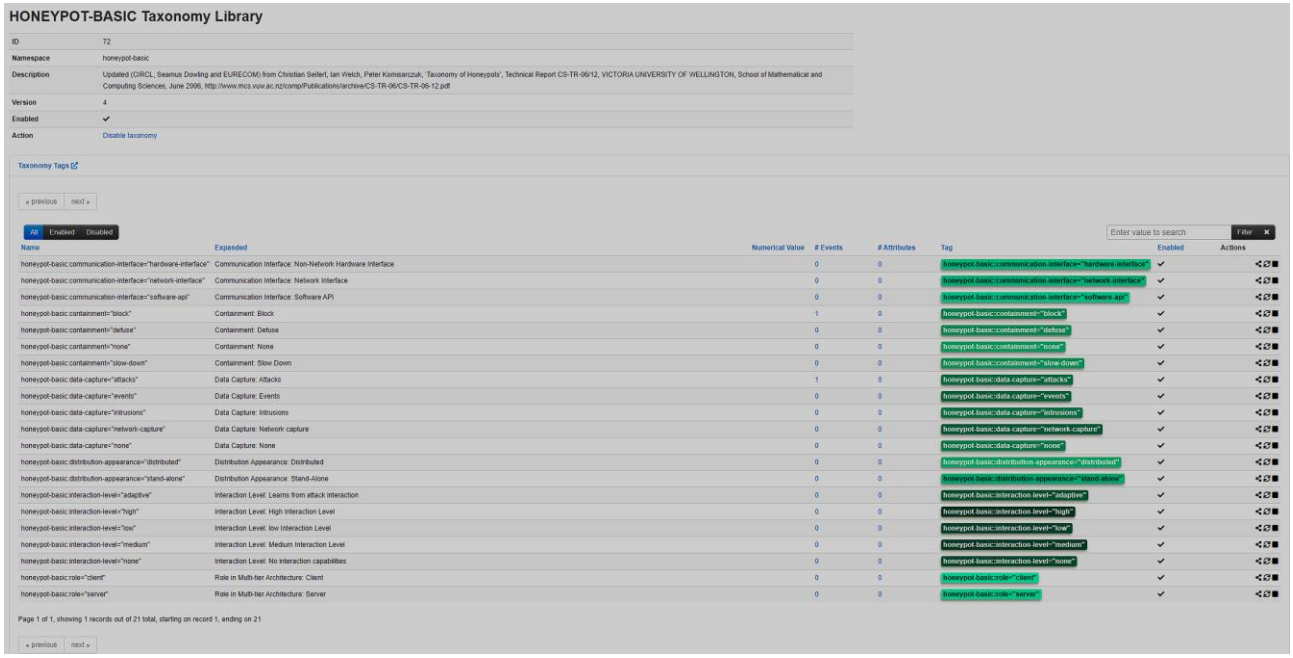


8 Minkä niminen tagi on merkitty ID-numerolla 600?

Botnet ”3101” on kyseinen tagi.

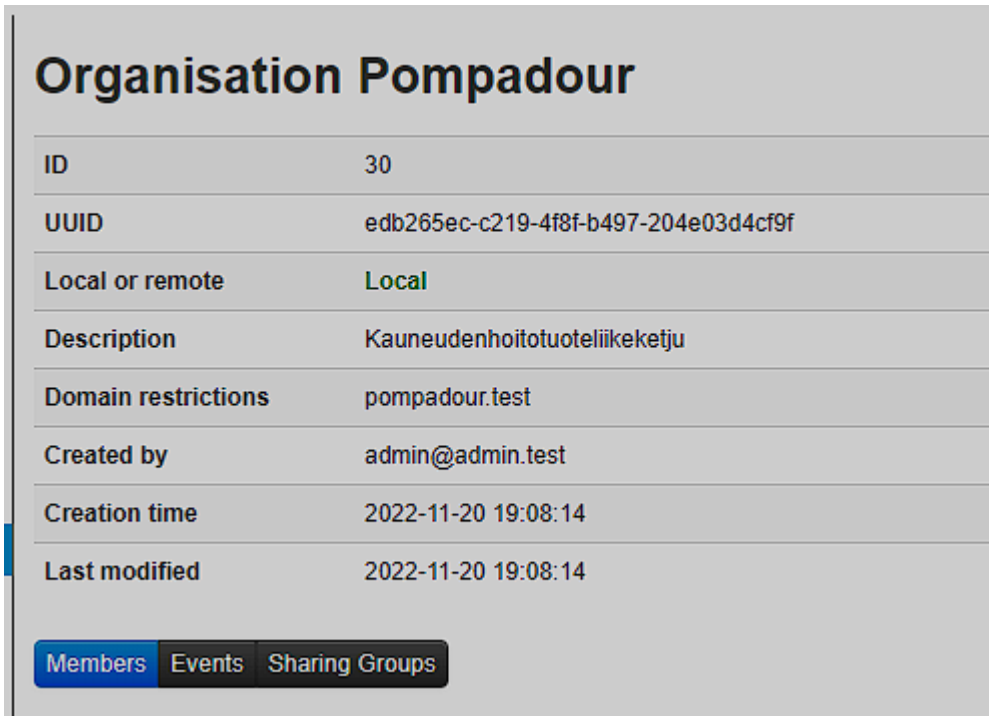
9 Minkä nimiset aktiiviset tagit ovat taksonomiakirjastossa honeypot-basic?





10 Mikä organisaatio on kaikista isoimmalla ID-numerolla järjestelmässä?

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



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.

Priority	Setting	Value	Description	Error Message
Critical	MISP.baseurl	https://misp.ttc60z.vle.fi	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	MISP.external_baseurl		The base url of the application (in the format https://www.mymispinstance.com) as visible externally/by other MISPs. 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 instnace 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	e239f6f6-51a5-4702-a869-56649dfaff93	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_publish_alert	true	The default setting for publish 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_paranoid	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_paranoid_skip_db	false	You can decide to skip the logging of the paranoid logs to the database.	
Critical	MISP.log_paranoid_include_post_body	false	If paranoid logging is enabled, include the POST body in the entries.	
Critical	MISP.log_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	MISP.proposals_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 recorrelation 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.ttc60z.vle.fi	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	MISP.external_baseurl		The base url of the application (in the format https://www.mymispinstance.com) as visible externally/by other MISPs. 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 instnace 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	e239f6f6-51a5-4702-a869-56649dfaff93	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_publish_alert	true	The default setting for publish 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_paranoid	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_paranoid_skip_db	false	You can decide to skip the logging of the paranoid logs to the database.	
Critical	MISP.log_paranoid_include_post_body	false	If paranoid logging is enabled, include the POST body in the entries.	
Critical	MISP.log_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	MISP.proposals_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 recorrelation 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 tähän lähdeluettelo.

Liitteet

Liite 1. Liitteen otsikko

Liite 2. Liitteen otsikko