



MISP järjestelmän tutkiminen

Ryhmä 13

Leevi Kauranen, AC7750

Samir Benjenna, AD1437

Eelis Suhonen, AA3910

Juho Eräjärvi, AD1276

Mikke Kuula, AC7806

Kyberuhkatieto ja data-analytiikka TTC6030-3011

02.12.2024

Tieto- ja viestintätekniikka

Sisältö

1	Johdanto.....	4
2	Järjestelmään tutustuminen.....	4
2.1	Jakeluasteet.....	4
2.2	Feedit	5
2.3	Nids sid -numero	5
2.4	MISP Attribuutit.....	6
2.5	Tapahtuma 1401.....	8
2.6	Varoitus- ja virheloki.....	10
2.7	Tunnisteet	10
2.8	Aktiiviset tunnisteet taksonomiakirjastossa	12
2.9	Organisaatiot.....	13
2.10	MISP serveriasetukset	14
	Lähteet	16

Kuviot

Kuvio 1.	Käyttäjän Esko.morko tiedot.....	6
Kuvio 2.	Search attribute -työkalun käyttö	7
Kuvio 3.	Attribuuttien määrä.....	7
Kuvio 4.	Tammi-pankki.....	8
Kuvio 5.	ID 1401, kalastelu viesti sisältää pahan linkin	9
Kuvio 6.	Hyökkäyksen tiedot	9
Kuvio 7.	MISP lokit	10
Kuvio 8.	Warnings and errors -filtteri.	10
Kuvio 9.	Tunnisteet	11
Kuvio 10.	Botnet	11
Kuvio 11.	Lisätietoja tunnisteesta.....	12
Kuvio 12.	Taksonomiat	12
Kuvio 13.	Taksonomian tunnisteet	13
Kuvio 14.	Suurin ID organisaatioilla	14

Kuvio 15. Yleiskatsaus serveriasetusten tilasta	14
Kuvio 16. Baseurl arvoa ei ole asetettu.....	15

1 Johdanto

Tässä harjoitustyössä tutustumme MISP (Malware Information Sharing Platform) järjestelmään. MISP on avoimen lähdekoodin tietoturvatyökalu. Sen avulla voidaan jakaa uhkatietoa ja sen avulla voidaan tehdä eri organisaatioiden ja yksityishenkilöiden välistä yhteistyötä tietoturvaan liittyvissä asioissa. MISPiin voi syöttää tietoa omista havaituista tietoturvauhkuista ja -tapahtumista ja tätä tietoa voidaan jakaa muille. MISPiä voidaan käyttää myös tietojen analysointiin. (Varsinainen asiantuntija. 2023).

2 Järjestelmään tutustuminen

Järjestelmään tutustuminen tapahtuu tutkimalla MISP:n jakeluasteita, feedejä, Nids sid -numeroita, attribuutteja, tapahtumia, lokeja, tunnisteita, taksonomiakirjastoa, organisaatiota ja serveriasetuksia.

2.1 Jakeluasteet

Kun MISP järjestelmään luodaan tapahtumaa, voidaan määritellä tapahtuman tietojen jakelun laajuus. Tämän avulla voidaan varmistua tiedon luottamuksellisuudesta ja jakamisen hallinnasta eri toimijoiden välillä.

Jakeluasteisiin kuuluu seuraavat:

- **Vain organisaatiosi:** tämä jakaa tapahtuman vain organisaation sisällä. Tämä jakeluaste valitaan, kun tiedot ovat erityisen arkaluonteisia tai luonteeltaan organisaatiokohtaisia.
- **Tämä yhteisö:** tiedot jaetaan vain kyseisessä MISP-järjestelmässä toimiville organisaatioille ja käyttäjille. Käytössä esimerkiksi tilanteessa, jossa tieto on arkaluontoista ja vastaanottajia täytyy rajoittaa
- **Yhteydessä olevat yhteisöt:** Tiedot jaetaan MISP-järjestelmää käyttäville yhteistyökumppaneille, jotka ovat suoraan yhteydessä palvelimeen. Käytössä esimerkiksi, kun tietoja halutaan jakaa laajemmalle yleisölle, mutta silti rajataan pääsy luotettaviin kumppaneihin
- **Manuaalinen (Sharing Group):** Tiedot jaetaan valituille ryhmille, joka koostuu käyttäjistä, organisaatioista tai muista palvelimista.

Distribution eli jakeluaste määrittää, miten feedejä jaetaan MISP-työkalussa. Voi pitää oman organisaation sisäisenä (Your Organisation only), MISP käyttäjille pelkästään (This Community Only), MISPiin liitetyille yhteisöille (Connected Communities) tai kaikille julkisesti (All Communities). Jakeluaste voidaan määritellä sen mukaan, onko tieto järkevää julkistaa, vai pitää organisaation sisäisenä, tai MISP sisäisenä. Jakeluasteen voi valita valikosta, kun on luomassa uutta feediä.

2.2 Feedit

MISP-järjestelmässä feed -osio on keskeinen ominaisuus, joka mahdollistaa automaattisen tiedon tuonnin ulkoisista lähteistä. Feedit ovat valmiita tietopaketteja, jotka sisältävät tietoturvaan liittyviä havaintoja, kuten tunnisteita ja uhkatietoja.

Tässä tapauksessa cybercrime-tracker.net toimittaa feedinsä freetext –muodossa.

Nettisivusto toimittaa feedin freetext muodossa, eli tekstiä ei ole välttämättä muotoiltu mitenkään, kuten CSV- tai JSON-tiedostomuotoihin.

Dashboard Galaxies Input Filters Global Actions **Sync Actions** Administration Logs API ★ MISP Admin Log out

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

Load default feed metadata Cache all feeds Cache freetext/CSV feeds Cache MISP feeds Fetch and store all feed data

« previous next »

Default feeds Custom feeds All feeds Enabled feeds

ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers	Target	Publish	Delta	Override	Distribution	Tag
6	✗	✗	cybercrime-tracker.net - all	freetext	cybercrime-tracker.net	network	https://cybercrime-tracker.net/all.php		Feed not enabled	✗	✓	✗	✗	Your organisation only	osint:source-...
35	✗	✗	http://cybercrime-tracker.net hashlist	freetext	http://cybercrime-tracker.net hashlist	network	https://cybercrime-tracker.net/ccamlist.php		Feed not enabled	✗	✗	✗	✗	Your organisation only	
36	✗	✗	http://cybercrime-tracker.net gatelist	freetext	http://cybercrime-tracker.net gatelist	network	https://cybercrime-tracker.net/ccamgate.php		Feed not enabled	✗	✗	✗	✗	Your organisation only	

2.3 Nids sid -numero

Tehtävänä on selvittää käyttäjän esko.morkon nids sid numero. Tämä löytyy, kun siirrymme organisations välilehdelle, ja valitsemme sieltä sivupalkista List Users. Kun haemme käyttäjää

Home | List Events | Dashboard | Settings | Import Filters | Object Actions | Sync Actions | Administration | Logs

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. For the value, event ID and organisation, you can enter several search terms by entering each term as a new line. To e For string searches (such as searching for an expression, tags, etc) - lookups are simple string matches. If you want a

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 ⁱ Category ⁱ

ALL ALL

☐ 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 ⁱ Last seen date ⁱ

2023-09-01 2024-04-01

First seen time ⁱ Last seen time ⁱ

HH:MM:SS.ssssss+TT:TT HH:MM:SS.ssssss+TT:TT

Expected format: HH:MM:SS.ssssss+TT:TT Expected format: HH:MM:SS.ssssss+TT:TT

Search

Kuvio 2. Search attribute -työkalun käyttö

Kun selaamme sivun pohjalle, selviää attribuuttien määrä, eli 54 kappaletta. (Kuvio 3)

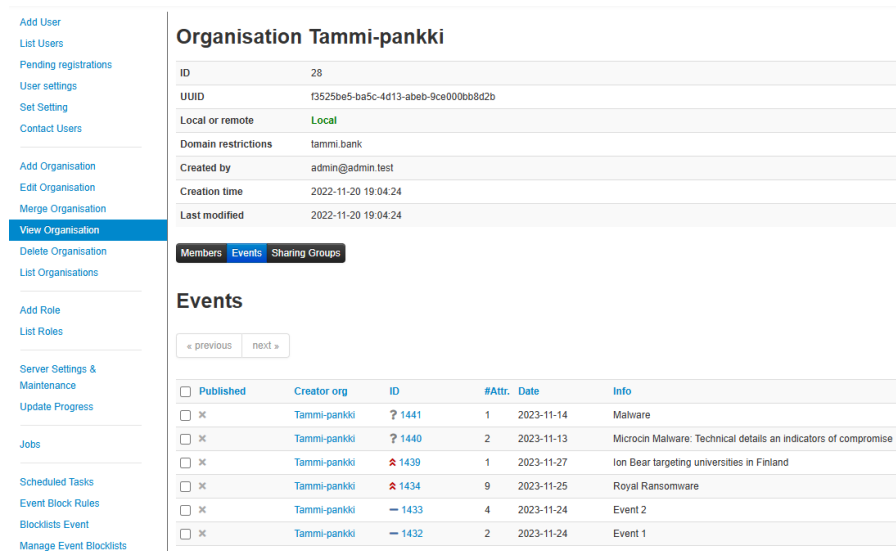
Year	ID	Organization	Type	Category	Value	Actions
2023-10-02	1401	Tammi-pankki	Person	first-name	Paul	
2023-09-13	1393	Tammi-pankki	Payload delivery	ip-src	192.168.1.100	
2023-09-05	1389	Pompadour	Other	text	Testi Attribuutti	
2023-09-05	1389	Pompadour	Internal reference	text	Tähäntunniste	
2023-09-05	1389	Pompadour	Other	text	Tinderfordummies	

Page 1 of 1, showing 54 records out of 54 total, starting on record 1, ending on 54

Kuvio 3. Attribuuttien määrä

2.5 Tapahtuma 1401

Seuraavaksi tarkastelemme tapahtumaa ID:n 1401 perusteella. Tämä tapahtuma on jaettu organisaation Tammi-pankki alle, joten siirrytään tarkastelemaan organisaatiota Tammi-pankki. (Kuvio 4).



Organisation Tammi-pankki

ID	28
UUID	f3525be5-ba5c-4d13-abe6-9ce000bb8d2b
Local or remote	Local
Domain restrictions	tammi.bank
Created by	admin@admin.test
Creation time	2022-11-20 19:04:24
Last modified	2022-11-20 19:04:24

Members Events Sharing Groups

Events

« previous next »

<input type="checkbox"/> Published	Creator org	ID	#Attr	Date	Info
<input type="checkbox"/> X	Tammi-pankki	? 1441	1	2023-11-14	Malware
<input type="checkbox"/> X	Tammi-pankki	? 1440	2	2023-11-13	Microcin Malware: Technical details an indicators of compromise
<input type="checkbox"/> X	Tammi-pankki	▲ 1439	1	2023-11-27	Ion Bear targeting universities in Finland
<input type="checkbox"/> X	Tammi-pankki	▲ 1434	9	2023-11-25	Royal Ransomware
<input type="checkbox"/> X	Tammi-pankki	— 1433	4	2023-11-24	Event 2
<input type="checkbox"/> X	Tammi-pankki	— 1432	2	2023-11-24	Event 1

Kuvio 4. Tammi-pankki

Tapahtuma 1401 löytyy Tammi-pankki –organisaation tapahtumista view organization ja sieltä events välilehdeltä kuvio 4 mukaan. Täältä voimme tarkastella eri tapahtumia ja niiden yksityiskohtia liittyen kyseiseen organisaatioon (kuvio 5).

Kalasteluviesti sisälsi pahan linkin

Event ID	1401
UUID	26ecdb88-9e40-4651-82c8-166856cbb897
Creator org	Tammi-pankki
Owner org	Tammi-pankki
Creator user	user25348@tammi.bank
Protected Event (experimental)	Event is in unprotected mode.
Tags	Download x Ransomware x tip:amber x cert-ist:threat_targeted_sector="Finance" x ecsirt:malicious-code="ransomware" x veris:actor:motive="Financial" x ms-caro-malware-full:malware-type="Ransom" x
Date	2023-10-02
Threat Level	High
Analysis	Initial
Distribution	This community only
Published	No
#Attributes	7 (1 Object)
First recorded change	2023-10-02 18:58:01
Last change	2023-10-02 19:21:25
Modification map	
Sightings	0 (0) - restricted to own organisation only

Kuvio 5. ID 1401, kalastelu viesti sisältää pahan linkin

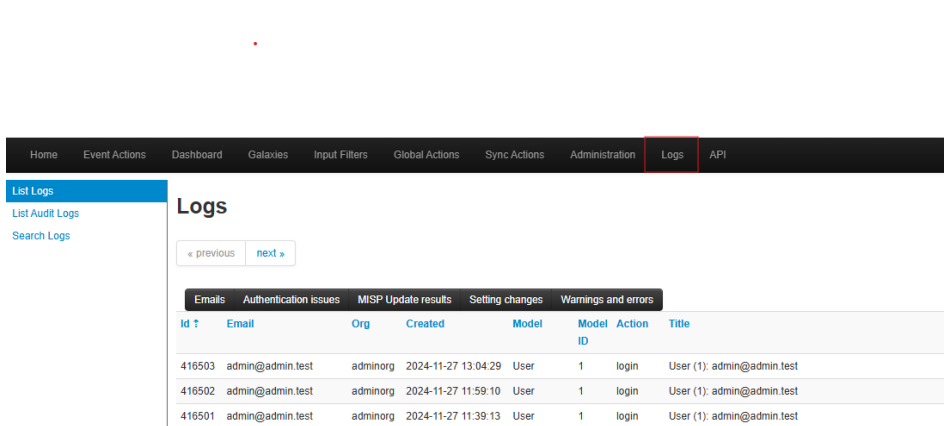
Kun selaamme tapahtumaa alaspäin, voimme nähdä lisätietoja tästä. Tässä tapauksessa löytyy esimerkiksi pahantekijän ransomwaren sisältävä tiedosto, joka oli liitettyä kalasteluviestiin sekä sha256-arvoja. Tiedoissa näkyy myös pankkitilin numero, jolle rahat oli tarkoitus laittaa. Pankkitilin numero on muotoa "OKOYFIHH", joten tästä voimme tutkia ja päätellä, että tapahtuman 1401 pahantekijä kuuluu mahdollisesti OP-pankin pankkiryhmään. (Kuvio 6).

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2023-10-02		Object name: file		file											
2023-10-02		Payload delivery	attachment	attachment											
2023-10-02		Payload delivery	file	file											
2023-10-02		Payload delivery	file	file											
2023-10-02		Network activity	file	file											
2023-10-02		Person	first-name	Paul											
2023-10-02		Financial fraud	iban	OKOYFIHH1234567891234567890											
2023-10-02		Payload delivery	file	file											

Kuvio 6. Hyökkäyksen tiedot

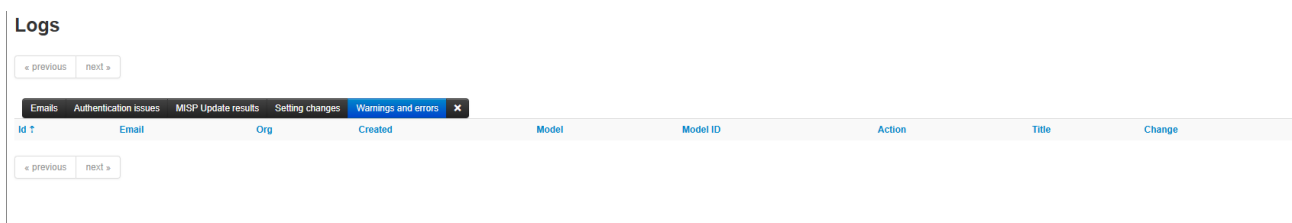
2.6 Varoitus- ja virheloki

Seuraavaksi tutkitaan MISP-järjestelmän loki osiota. (Kuvio 7)



Kuvio 7. MISP lokit

Tehtävän tarkoitus on selvittää, kuinka monta virhettä varoitus- ja virhelokissa on. Saamme tämän selvitettyä valitsemalla Warnings and errors -filtterin. Kuviosta 8 selviää, että lokeissa ei ole yhtään virhe- tai varoituslokiä.



Kuvio 8. Warnings and errors -filtteri.

2.7 Tunnisteet

Tutkitaan seuraavaksi tags välilehteä, jolta löydämme erinäisiä tapauksissa käytettyjä "tageja" eli tunnisteita. Tehtävä on etsiä tunniste, jonka id on 600.

Siirrytään kuvion 9 mukaisesti Tags-välilehdelle, jolle on listattu käytettyjä tunnisteita.

Tags

< previous 1 2 3 4 5 6 7 next > last >

Sample	Advanced	Exportable	Hidden	Local Only	Name	Restricted to org	Restricted to user	Taxonomy	Favourite	Actions
479	✓	✓	✓	✓	malware_classification:malware category="Botnet"	✓	✓		<input type="checkbox"/>	
388	✓	✓	✓	✓	C2	✓	✓		<input type="checkbox"/>	
423	✓	✓	✓	✓	Cobalt Strike Beacon	✓	✓		<input type="checkbox"/>	
417	✓	✓	✓	✓	SQL Drapper	✓	✓		<input type="checkbox"/>	
420	✓	✓	✓	✓	Drone	✓	✓		<input type="checkbox"/>	
421	✓	✓	✓	✓	DocBot	✓	✓		<input type="checkbox"/>	
416	✓	✓	✓	✓	Downstat	✓	✓		<input type="checkbox"/>	
511	✓	✓	✓	✓	Flash	✓	✓		<input type="checkbox"/>	
924	✓	✓	✓	✓	Malicious Dutch Script	✓	✓		<input type="checkbox"/>	
907	✓	✓	✓	✓	Remnuxware	✓	✓		<input type="checkbox"/>	
384	✓	✓	✓	✓	Snake Loader	✓	✓		<input type="checkbox"/>	
305	✓	✓	✓	✓	SQL Injections	✓	✓		<input type="checkbox"/>	
740	✓	✓	✓	✓	"Lingender Limited"	✓	✓		<input type="checkbox"/>	
636	✓	✓	✓	✓	SQL Injection	✓	✓		<input type="checkbox"/>	
891	✓	✓	✓	✓	WordPress Admin	✓	✓		<input type="checkbox"/>	
537	✓	✓	✓	✓	SQL	✓	✓		<input type="checkbox"/>	
35	✓	✓	✓	✓	SQL	✓	✓		<input type="checkbox"/>	
633	✓	✓	✓	✓	ARTE.DA CONSULTING LIMITED	✓	✓		<input type="checkbox"/>	
562	✓	✓	✓	✓	Actor: APT28	✓	✓		<input type="checkbox"/>	
543	✓	✓	✓	✓	Actor: Lazarus	✓	✓		<input type="checkbox"/>	

Kuvio 9. Tunnisteet

Etsitään tunnisteista id numeroa 600. Kuviosta 10 käy ilmi, että kyseinen tunniste kuuluu Botnet "3101":lle.

236	✓	✓	✓	✓	Banker	✓	✓	2	0	<input type="checkbox"/>
599	✓	✓	✓	✓	Banker: Dridex	✓	✓	1	0	<input type="checkbox"/>
598	✓	✓	✓	✓	Banker: Gozi ISFB v2	✓	✓	1	0	<input type="checkbox"/>
579	✓	✓	✓	✓	Banker: TrickBot	✓	✓	4	1	<input type="checkbox"/>
384	✓	✓	✓	✓	Botbot	✓	✓	1	0	<input type="checkbox"/>
600	✓	✓	✓	✓	Botnet "3101"	✓	✓	1	0	<input type="checkbox"/>
597	✓	✓	✓	✓	CERT.XLM-malicious-code="spyware-rai"	✓	✓	3	0	<input type="checkbox"/>
731	✓	✓	✓	✓	CERT.XLM-malicious-code="trojan-malware"	✓	✓	1	0	<input type="checkbox"/>
538	✓	✓	✓	✓	CHCHES	✓	✓	0	27	<input type="checkbox"/>
1901	✓	✓	✓	✓	CTIA kill chain:C2	✓	✓	1	4	<input type="checkbox"/>

Kuvio 10. Botnet

Tunniste on Botnet. Löytyi Event Actions -> List Tags, kun avaa jako napista kyseisen Eventin, näkee graafisena esityksenä, miten Tag ja Event liittyvät toisiinsa kuva. (Kuvio 11).





Kuvio 11. Lisätietoja tunnisteesta

2.8 Aktiiviset tunnisteet taksonomiakirjastossa

Siirrytään seuraavaksi Event Actions osion alta List Taxonomies osuuteen. Tehtävänä on etsiä ho-
neypot-basic taksonomian aktiiviset tunnisteet.

Etsitään honeypot-basic taksonomia haulla. (Kuvio 12).

Taxonomies									
« previous		next »							
All		Enabled		Disabled					
						honeypot-basic			
						Filter			
ID ↑	Namespace	Description	Version	Enabled	Required	Active Tags	Actions		
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, http://www.mcs.vuw.ac.nz/comp/Publications/archive/CS-TR-06/CS-TR-06-12.pdf	4	✖	<input type="checkbox"/>	2 / 21	 		

Kuvio 12. Taksonomiat

Kun avaamme taksonomian, näemme aktiiviset tunnisteet. (Kuvio 13).

Taxonomy Tags

« previous next »

Enter value to search

Name	Expanded	Numerical Value	# Events	# Attributes	Tag	Enabled	Actions
honeypot-basic:communication-interface="hardware-interface"	Communication Interface: Non-Network Hardware Interface	0	0			N/A	
honeypot-basic:communication-interface="network-interface"	Communication Interface: Network Interface	0	0			N/A	
honeypot-basic:communication-interface="software-api"	Communication Interface: Software API	0	0			N/A	
honeypot-basic:containment="block"	Containment: Block	1	0		honeypot-basic:containment="block"	✓	
honeypot-basic:containment="defuse"	Containment: Defuse	0	0			N/A	
honeypot-basic:containment="none"	Containment: None	0	0			N/A	
honeypot-basic:containment="slow-down"	Containment: Slow Down	0	0			N/A	
honeypot-basic:data-capture="attacks"	Data Capture: Attacks	1	0		honeypot-basic:data-capture="attacks"	✓	
honeypot-basic:data-capture="events"	Data Capture: Events	0	0			N/A	
honeypot-basic:data-capture="intrusions"	Data Capture: Intrusions	0	0			N/A	
honeypot-basic:data-capture="network-capture"	Data Capture: Network capture	0	0			N/A	
honeypot-basic:data-capture="none"	Data Capture: None	0	0			N/A	

Kuvio 13. Taksonomian tunnisteet

2.9 Organisaatiot

MISP-järjestelmässä organisaatiot edustavat yksittäisiä toimijoita, jotka jakavat uhkatietoa. Ne voivat olla esimerkiksi yrityksiä, tietoturvaorganisaatioita, viranomaisia tai tutkimuslaitoksia. Järjestelmän organisaatorakenne auttaa hallitsemaan tiedon omistajuutta, pääsyoikeuksia ja jakeluasetuksia.

Tehtävänä on selvittää organisaatio, jolla on suurin ID-numero. Siirrytään Global Actions lehden alta organisations osioon. Täältä valitsemme all organisations ja suodatamme laskevasti ID-numeron mukaan. Suurin ID-numero löytyy siis yritykseltä DEMO-ORG. (Kuvio 14).

All organisations having a presence on this instance

◀ previous next ▶

[+ Add](#)
[Local organisations](#)
[Known remote organisations](#)
[All organisations](#)

Enter value to search Filter

ID ↑	Name	UUID	Description	Nationality	Sector	Type	Contacts	Added by	Local	Users	Restrictions	Actions
35	DEMO-ORG	5c1eb4f8-bae5-45f5-a772-96d4a3f54c3e						admin@admin.test	✗	0		🔍 🗑️
34	ICS-CSIRT.io	019e8d5f-83da-4d59-982d-e94cdcc7dbc7						admin@admin.test	✗	0		🔍 🗑️
33	CUDESO-PRIV	5e1b7d20-bbbc-456e-b270-479b29b8f09f						admin@admin.test	✗	0		🔍 🗑️
32	CUDESO	56c42374-fdb8-4544-a218-41fbc0a8ab16						admin@admin.test	✗	0		🔍 🗑️
31	THA-CERT	58a4d347-8460-4fc7-a882-6728c0a82ae5						admin@admin.test	✗	0		🔍 🗑️
30	Pompadour	edb265ec-c219-488f-b497-204e03d4c9f	Kauneudenhoitotuotetietokehitys					admin@admin.test	✓	24	pompadour.test	🔍 🗑️
29	Bisyklic	419042ce-62fe-44c5-95f7-9396b67e8c87	Polkupyörävalmistaja Bisyklic					admin@admin.test	✓	27	bisyklic.bike	🔍 🗑️
28	Tammi-pankki	f3525be5-ba5c-4d13-abeb-9ce000bb8d2b						admin@admin.test	✓	43	tammi.bank	🔍 🗑️
27	02	372a7b2b-4379-4007-8201-a39ef883dd08	Group 2					admin@admin.test	✓	0		🔍 🗑️
26	BSK	56024f6c-da70-4584-b689-48ef950d210f						admin@admin.test	✗	0		🔍 🗑️
25	SCTIF	5a313608-0410-4941-aaeb-8607950d210f						admin@admin.test	✗	0		🔍 🗑️
24	CERT-FR_1510	56bd779-46f8-4353-bd09-2be95bce2212						admin@admin.test	✗	0		🔍 🗑️
23	Centre for Cyber security Belgium	5cfd6e53-b5f8-43e7-be9a-49880a3b4631						admin@admin.test	✗	0		🔍 🗑️
22	The DFIR Report	5e9e5d86-b094-4f6-b07e-4e3e950d210f						admin@admin.test	✗	0		🔍 🗑️
21	laskowski-tech.com	5e157d76-c92c-4acd-a54e-4a01950d210f						admin@admin.test	✗	0		🔍 🗑️
20	wilbursecurity.com	5e16d2bc-5c58-4ef1-bc80-47f5950d210f						admin@admin.test	✗	0		🔍 🗑️
19	MISOC	5d49b744-1ef4-4480-b486-40f0b08ac45						admin@admin.test	✗	0		🔍 🗑️
18	Heslat	5cb1fe4f-5ebc-4dc2-b79f-4374b49ab0f9						admin@admin.test	✗	0		🔍 🗑️
17	citizenlab	581b5faa-818c-441a-bd1d-49798e96ca05						admin@admin.test	✗	0		🔍 🗑️
16	VK_INTEL_EVIL	5d2fbc3a-e520-4b09-89b7-1b0a6b09e8cf						admin@admin.test	✗	0		🔍 🗑️
15	MalwareMustDie	569e04b2-ef00-45bd-b83a-47fb950d210f						admin@admin.test	✗	0		🔍 🗑️
14	FIIRY FA	5cde77cfd4-bcda-4a76-8045-f17c7c7a0b16a						admin@admin.test	✗	0		🔍 🗑️

Kuvio 14. Suurin ID organisaatioilla

2.10 MISP serveriasetukset

Viimeisenä selvitämme MISP-serveriasetusten tilaa ja löytyykö palvelimelta kriittisesti vioittuneita asetuksia.

Kuviossa 15 näemme kaikkien asetusten kokonaiskuvan. Listassa on kaksi riviä punaisella, toinen kuvastaa MISP asetusten kokonaistilaa, ja toinen ilmoittaa 7 väärin tehdystä asetuksesta.

Server Settings & Maintenance

[Overview](#)
[MISP \(13 ⚠️\)](#)
[Encryption \(7 ⚠️\)](#)
[Proxy \(5\)](#)
[Security \(7 ⚠️\)](#)
[Plugin \(537 ⚠️\)](#)
[SimpleBackgroundJobs](#)
[Correlations](#)
[new](#)
[Diagnostics](#)
[Manage files](#)
[Workers](#)

Test	Value	Description
Overall health	Critical, your MISP instance requires immediate attention.	The overall health of your instance depends on the most severe unresolved issues.
Critical settings incorrectly or not set	7 incorrect settings.	MISP will not operate correctly or will be insecure until these issues are resolved.

Kuvio 15. Yleiskatsaus serveriasetusten tilasta

Kun siirrymme MISP välilehdelle katsomaan MISP-asetuksia, löytyy sieltä 1 rivi punaisella, joka viestii MISP-external_baseurl asetuksen puutteellisesta arvosta. (Kuvio 16).

Server Settings & Maintenance

Overview				Filter the table(s) below	
Priority	Setting	Value	Description	Error Message	
Critical	MISPbaseurl	https://misp.ttu50z.vie.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	MISPexternal_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.	

Kuvio 16. Baseurl arvoa ei ole asetettu

Lähteet

Varsinainen asiantuntija. No mikäs on Misp?. 1.11.2023. Artikkelit kyberiakysymyksia.com sivustolla. Viitattu 2.12.2024. <https://kyberiakysymyksia.com/2023/11/no-mikas-on-misp/>.