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](#_Toc184037363)

[2 Järjestelmään tutustuminen 4](#_Toc184037364)

[2.1 Jakeluasteet 4](#_Toc184037365)

[2.2 Feedit 5](#_Toc184037366)

[2.3 Nids sid -numero 6](#_Toc184037367)

[2.4 MISP Attribuutit 6](#_Toc184037368)

[2.5 Tapahtuma 1401 8](#_Toc184037369)

[2.6 Varoitus- ja virheloki 11](#_Toc184037370)

[2.7 Tunnisteet 11](#_Toc184037371)

[2.8 Aktiiviset tunnisteet taksonomiakirjastossa 13](#_Toc184037372)

[2.9 Organisaatiot 15](#_Toc184037373)

[2.10 MISP serveriasetukset 15](#_Toc184037374)

[Lähteet 17](#_Toc184037375)

Kuviot

[Kuvio 1. Käyttäjän Esko.morko tiedot 6](#_Toc184037347)

[Kuvio 2. Search attribute -työkalun käyttö 7](#_Toc184037348)

[Kuvio 3. Attribuuttien määrä 8](#_Toc184037349)

[Kuvio 4. Tammi-pankki 9](#_Toc184037350)

[Kuvio 5. ID 1401, kalastelu viesti sisältää pahan linkin 10](#_Toc184037351)

[Kuvio 6. Hyökkäyksen tiedot 10](#_Toc184037352)

[Kuvio 7. MISP lokit 11](#_Toc184037353)

[Kuvio 8. Warnings and errors -filtteri. 11](#_Toc184037354)

[Kuvio 9. Tunnisteet 12](#_Toc184037355)

[Kuvio 10. Botnet 12](#_Toc184037356)

[Kuvio 11. Lisätietoja tunnisteesta 13](#_Toc184037357)

[Kuvio 12. Taksonomiat 13](#_Toc184037358)

[Kuvio 13. Taksonomian tunnisteet 14](#_Toc184037359)

[Kuvio 14. Suurin ID organisaatioilla 15](#_Toc184037360)

[Kuvio 15. Yleiskatsaus serveriasetusten tilasta 16](#_Toc184037361)

[Kuvio 16. Baseurl arvoa ei ole asetettu 16](#_Toc184037362)

# 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 tietoturvauhkista ja -tapahtumista ja tätä tietoa voidaan jakaa muille. MISPiä voidaan käyttää myös tietojen analysointiin. (Varsinainen asiantuntija. 2023).

# Järjestelmään tutustuminen

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

## 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.

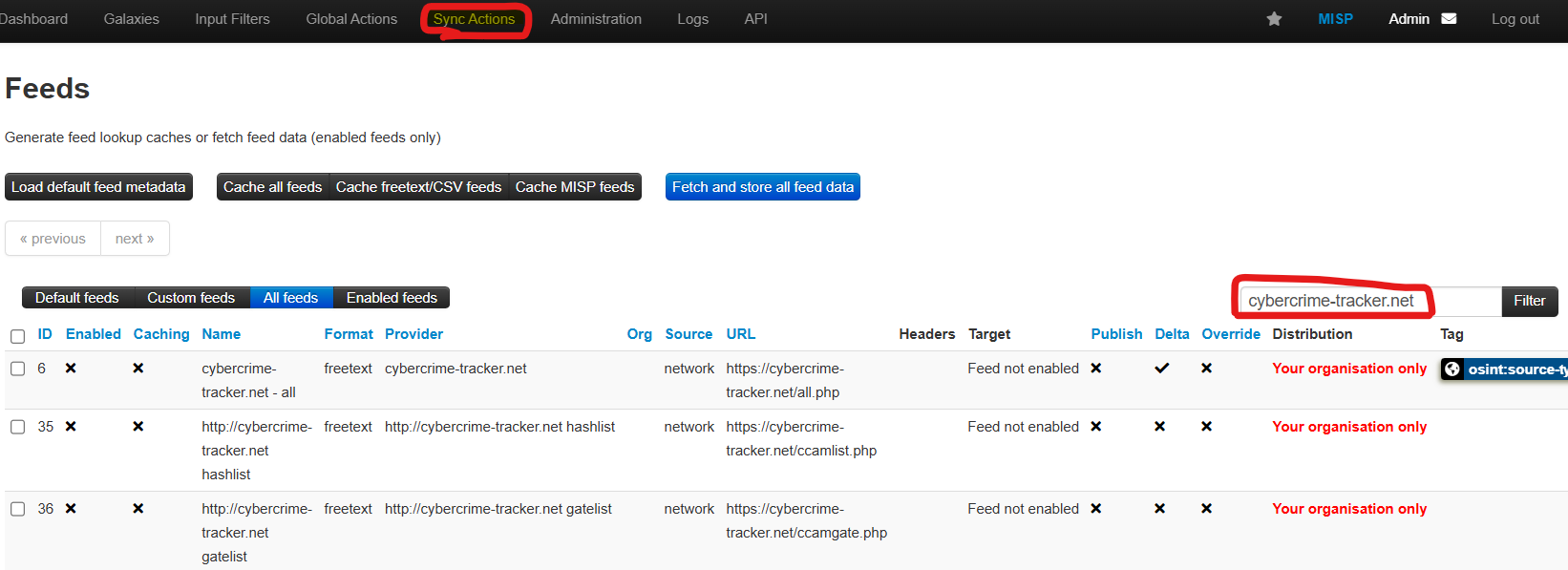
Distribution eli jakeluaste määrittää, miten feedejä jaetaan MISP-työkalussa. Voi pitää oman organisaation sisäisenä (Your Organisation only), MISP käyttäjille pelkästään (This Community Only), MISPiin liitetyille yhteisöille (Connected Communities) tai kaikille julkisesti (All Communities). Jakeluaste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

## 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.



## 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 esko.morko, saamme selville käyttäjän tiedot. (Kuvio 1) Tiedoista selviää, että käyttäjän NIDS SID -numero on 5706234.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuvio 1. Käyttäjän Esko.morko tiedot

## MISP Attribuutit

MISP-järjestelmästä löytyy osiot list attributes ja search attributes. Nämä attribuutit ovat tapahtumien (events) osia, jotka kuvaavat yksityiskohtaisia uhkatietoja. Näitä voi olla esimerkiksi tekniset indikaattorit, kuten haittaohjelman hash tai IP-osoite.

Tehtävän tarkoitus on saada selville aikavälin 1.9.2023-1.3.2024 attribuuttien määrä.

Tämä selviää, kun siirrymme Event Actions lehden alle Search Attributes osioon, ja sieltä etsimme aikavälillä esiintyvät attribuutit kuvion 2 mukaisesti.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

Kuvaus luotu automaattisesti

Kuvio 2. Search attribute -työkalun käyttö

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

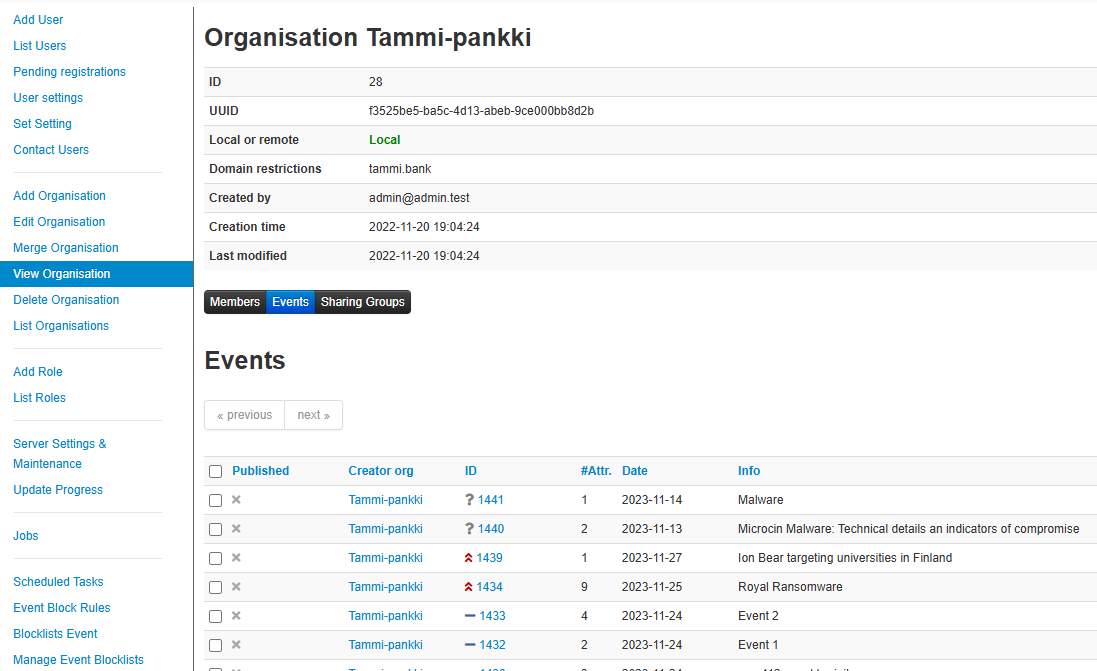
Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

Kuvio 3. Attribuuttien määrä

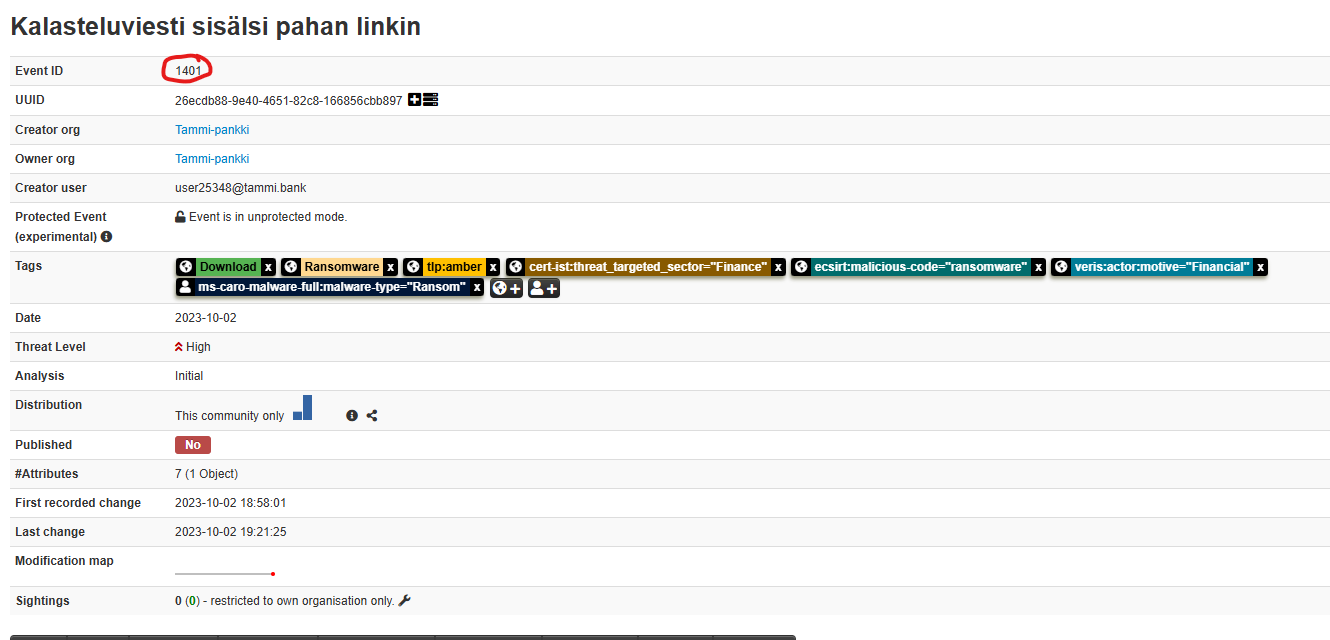
## Tapahtuma 1401

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



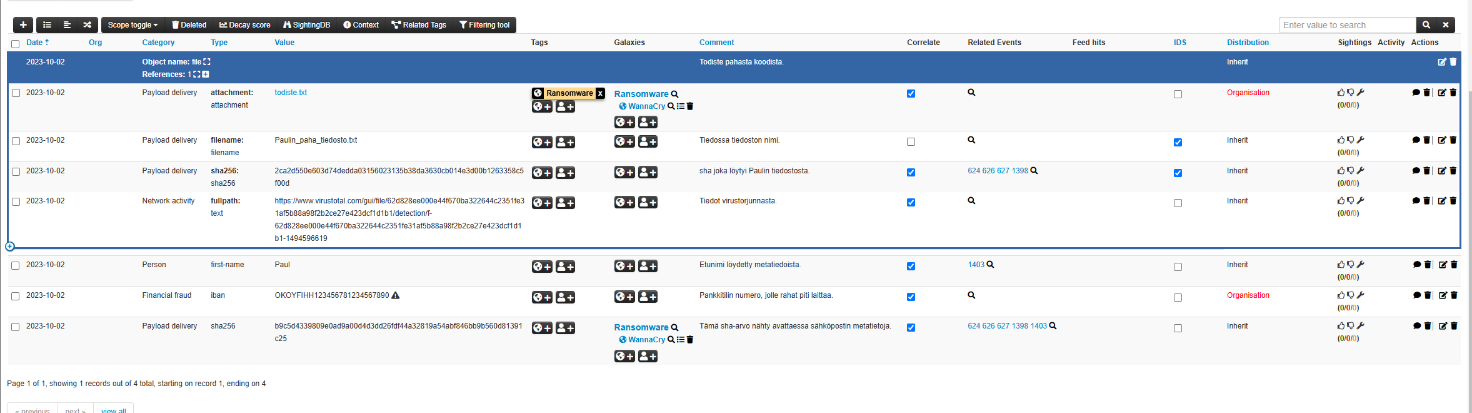
Kuvio 4. Tammi-pankki

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).



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 liitettynä 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).



Kuvio 6. Hyökkäyksen tiedot

## Varoitus- ja virheloki

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Verkkosivusto

Kuvaus luotu automaattisesti

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 varoituslokia.

Kuva, joka sisältää kohteen teksti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 8. Warnings and errors -filtteri.

## 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.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, numero, ohjelmisto

Kuvaus luotu automaattisesti

Kuvio 9. Tunnisteet

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

Kuva, joka sisältää kohteen kuvakaappaus, teksti, viiva, numero

Kuvaus luotu automaattisesti

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

## Aktiiviset tunnisteet taksonomiakirjastossa

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

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus

Kuvaus luotu automaattisesti

Kuvio 12. Taksonomiat

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

Kuva, joka sisältää kohteen teksti, kuvakaappaus, numero, Fontti

Kuvaus luotu automaattisesti

Kuvio 13. Taksonomian tunnisteet

## Organisaatiot

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

Tehtävänämme 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).

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, numero

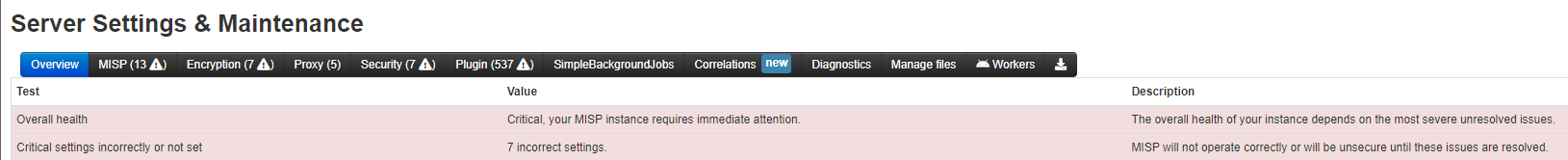
Kuvaus luotu automaattisesti**

Kuvio 14. Suurin ID organisaatioilla

## MISP serveriasetukset

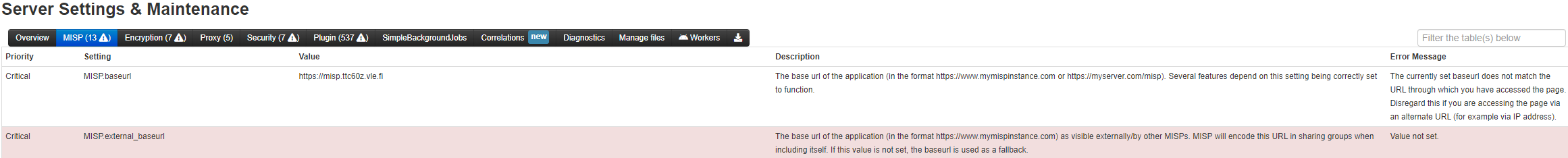
Viimeisenä selvitämme MISP-serveriasetusten tilaa ja löytyykö palvelimelta kriittisesti vioittuneita asetuksia.

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



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).



Kuvio 16. Baseurl arvoa ei ole asetettu

Lähteet

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