

MISP

MISP är en plattform för att dela säkerhetsrelaterad information (så som t.ex. IOCer) på ett strukturerat sätt. Det förenklar import & export av data, som i sin tur underlättar automation baserat på data.

SUNET har en MISP-instans under som ligger under SUNET CERT, som alla SUNET-anslutna organisationen kan få access till samt ansluta sin lokala MISP-instans samt.

MISP användarpolicy

Åtkomst

För att kunna nyttja MISP-tjänsten måste man vara SWAMID-medlem och ha en IdP (det är endast federerad inloggning som stöds av SUNETs MISP-instans).

För att få sitt konto aktiverat i MISP-instansen måste man säkra att användarens IdP släpper eppn-attributet till MISP-SPn. Efter det kan användaren göra en första inloggning mot MISP-SPn (via <https://misp.cert.sunet.se>) och sedan meddela sin lokala IRT-ansvarige, så att hen kan aktivera kontot i MISP:en. (Tills kontot inte aktiverats så kommer du få ett felmeddelande likt "för många redirects gjordes..." (pga att man inte släpps in av MISP:en))

Vilken säkerhetsrelaterad information efterfrågas i första hand av CERT/CSIRT/IRT-grupperna?

- Information kring phishing-försök, (t.ex. URL:er, domännamn, epost-avsändare, osv.)
- Malware data (t.ex. C&C servrars IP-adresser, hashar osv.)
- Källor som gör intrångsförsök (t.ex. IP-adresser)

Vilken information bör man dela med sig av?

- *En upprepning av svaren i föregående fråga*

Hur bör data man delar med sig av struktureras upp?

- För att andra enklare ska kunna använda sig av data som man delar med sig av, krävs åtminstone viss klassifiering:
 1. Informations säkerhetsklassning: **TLP** (t.ex. "**TLP:white**")
 2. Händelsetyp: **ENISA RTIS** (t.ex. "**Malicious Code**")
 3. Tillitsfaktor på data (gruppindelning inte beslutad, förslag?)
*Tills detta inte är beslutat, föreslås att endast händelser med data av högsta tillitsfaktor bör läggas in och även sätta **IDS-flaggan** så andra kan använda det för automatisering.*

Tidigare MISP workshop

2019 hade SUNET tillsammans med [CIRCL](#) anordnat en workshop kring MISP. Allt det materialet finns publicerat [här](#).