MISP

MISP är en platform för att dela säkerhetsrelaterad information (så som t.ex. IOCer) på ett strukturerar sätt för att underlätta import/export av strukturerad data för att underlätta automation. SUNET har en MISP-instans under SUNET CERT som alla SUNET-anslutna organisationen kan ansluta emot.

MISP workshop

Tidigare i år så hade SUNET tillsammans med CIRCL en workshop kring MISP. Allt material finns publiserat här.

Om intresse finns kanske vi skulle kunna göra det igen vid senare tillfälle, men troligast först nästa år (2020).

MISP användarpolicy

Åtkomst

För att kunna nyttja tjänsten bör man vara SWAMID-medlem och ha en egen IdP (det är endast federerad inloggning till MISP-instansen). För att få sitt inloggningskonto aktiverat i MISP-instansen måsta man först logga in en gång (via https://misp.cert.sunet.se) och sedan meddela pettai vilket EPPN (format: uid@realm), så kontot kan aktiveras.

Tills kontot inte aktiverats så kommer man få ett felmeddelande likt "för många redirects gjordes..." (pga att man inte släpps in i MISPen)

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

- Information kring phishing-försök, domäner, osv.
- Malware data osv.
- Källor som gör intrångsförsök

Vilken information bör man dela med sig av?

- En upprepning av föregående rubrik / frågeställning

Hur bör datat man delar med sig av struktureras upp?

- För att andra enklare ska kunna använda sig av datat som man delar med sig av, krävs åtminstone viss klassifiering:
    1. Informationsäkerhetsklassning: **TLP** (t.ex. "***TLP:white***")
    2. Händelsetyp: **ENISA RTIS** (t.ex. "***Malicious Code***")
    3. Tillitsfaktor på datat (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.*