MISP BoF, SUNET-dagarna

Vi har haft en MISP BoF på SUNET-dagarna, där följande riktlinjer för informationdelning via MISP föreslogs:

Vilken information skulle vi vilja få delad?

- Phishing
- Malware

Vilken information skulle vi kunna tänka dela med oss av?

- Phishing
- Malware

Vilken Taxonomier bör vi använda?

- Informationsklassifiering på informationen **TLP**
- Klassifiering på typen av händelse **ENISA RTIS**
- Hur tillförlitlig är materialet i händelsen i första hand bara dela det mest tillförlitliga datat (samt lägga på IDS -flaggan för attribut att automatisera på)