

A MISP instance for WLCG

WLCG GDB, 14th Sept 2016

R. Wartel, CERN





The problem

- Malware and attacks global
 - Largely evade intrusion detection systems, filters, etc.
 - Details on most common techniques during the WLCG Workshop
- Typical WLCG/HEP/private organisation:
 - No free time or expertise to look into ongoing malicious trends
 - Just want to know what to look for, block or investigate further
- Great amount of knowledge and expertise available
 - Security vendors, security teams, law enforcement, etc.
 - Need to collaborate
 - CERN: contacts at other organisations our #1 IDS for many years
- “Threat intelligence” is now a key field of computer security



MISP

- Main challenge: get quality/actionable “threat intelligence”
 - Involves building contacts and trust relationships
- MISP: “Malware Information Sharing Platform”
 - <http://www.misp-project.org/>
 - Used by many security teams and security communities
 - Does not solve the trust issues — This is just a tool to share data
- **WLCG Security Operations Center (SOC) WG**
 - Discussed this tool already
 - Several sites are actively evaluating MISP
 - GridPP seems for example well advanced!



CERN MISP

- CERN happy to run a central MISP instance for WLCG/HEP
 - Enable **sites to share or simply pull** data for their own use
 - Enable direct sharing with **other MISP instances**
 - Share threat intelligence gathered by the CERN Security Team from **other sources** (when authorised)
- Two main goals:
 - Be **quicker** than vendors can update their tool currently
 - Share sensitive or confidential intelligence automatically
- Two ways to access the CERN MISP instance:
 - Web portal
 - Authentication by eduGAIN (with Sirtifi + R&S)
 - Authorization by e-groups
 - API access (with API key to pull data automatically)



Quick demo

CERN Authentication

https://login.cern.ch/adfs/ls/?wa=wsignin1.0&wreply=https%3A%2F%2Fmisp.cern.ch%2FShibboleth.sso%2FADF...

CERN Accelerating science Sign in Directory

CERN Single Sign-On

Sign in with a CERN account, a Federation account or a public service account

Sign in with your CERN account

Reminder: you have agreed to comply with the [CERN computing rules](#)


Use credentials


Username or Email address Password Sign in

Remember Username or Email Address [Need password help?](#)

Password is required


Use one-click authentication

 [Sign in using your current Windows/Kerberos credentials \[autologon\]](#)
Use your current authentication token. You need Internet Explorer on CERN Windows or Firefox on SLC ([Firefox help here](#)).

 [Sign in using your Certificate \[autologon\]](#)
Use a EuGridPMA trusted certificate. Don't forget to first map your Certificate to your CERN Account.

Use strong two factor authentication [show]

Sign in with a public service account

 [Facebook, Google, Live, etc.](#)
Authenticate using an external account provider such as Facebook, Google, Live, Yahoo, Orange.

Sign in with your organization or institution account





Key issues

- Ultimate goal:
Bring high quality threat intelligence to all WLCG partners
 - Liaising with more infrastructures and communities
 - Reduce false positives and improve relevance
- Easy to set up a MISP instance... but then what?
 - Correlation with local logs and data non trivial
 - No easy strategy, solutions likely site-dependent
 - We must invest more time/resources in the SOC WG
 - “Campus” security and “grid” security must work together