WLCG Security Working Groups

David Crooks
david.crooks@glasgow.ac.uk

on behalf of
WLCG Traceability & Isolation WG
WLCG Security Operations Centres WG

WLCG Workshop, October 2016

Security Working Groups

- Earlier this year, two WLCG security working groups were established
- Follow on from Cloud Traceability TF
  - Traceability & Isolation (Vincent Brillault)
  - Security Operations Centres (Liviu Vâlsan, David Crooks)

Traceability & Isolation

- “Explore new traceability and isolation paradigms, propose a new model taking advantage of new technologies and VO frameworks while keeping full trustworthy traceability and isolation of users actions.”

Traceability

- One initial step has been to look at the traceability logging information stored by VOs (and associated frameworks)

- *VOs did not identify any blocking issues with their traceability logging*

- *They can identify users and the associated payload that run jobs on a worker node during a given period of time*

Isolation

- On the other track, the group is looking at technologies to provide isolation

- *An existing solution for daemon-less containers has been identified: Singularity [singularity.lbl.gov]*

- *Requires SUID on RHEL7.3 but not upstream kernels; a transition measure could be to support it on RHEL 7.3 as a SUID and then remove the SUID as soon as the RedHat kernel supports unprivileged mount namespaces*

Next steps

- *Sites are still encouraged to join the working group*
- *Especially to express their needs with regard to a new traceability model where they have to rely on VO to do the final traceability*

Security Operations Centres

- Security & Analytics
- *"Establish a clear set of desired data outputs and necessary inputs.*
- *Create a scalable reference design applicable for a range of sites by examining current and prospective SOC projects & tools."*

Strategy

- Start with specific tools and grow our understanding and requirements

- New area of work - challenges include engaging with all the appropriate security teams and stakeholders

Framework

Minimum viable product

- MISP Threat Intelligence sharing
  [misp-project.org]
- Bro Network Security Monitor
  [bro.org]

Reference design

- Metron Security Operations Centre
  [metron.incubator.apache.org]

Status

- MISP tested at GridPP sites in test configuration to explore data sharing in controlled way
- Bro testing in progress, looking at traffic capture and analysis
- WLCG MISP instance [Romain Wartel]
- Presentation on ZNeTS2

Next steps

- Continue work on individual components
  - Integration within components: MISP + Bro
- Welcome more involvement from sites, particularly those who could help with testing in different contexts and environments and those with existing tools

Contact

- *wlcg-traceability-isolation-wg@cern.ch*
- *https://wlcg-traceability-isolation-wg.web.cern.ch*
- *wlcg-soc-wg@cern.ch*
- *https://wlcg-soc-wg.web.cern.ch*