Security Operations Centre WG

pre-GDB report

David Crooks

wlcg-soc-wg@cern.ch

GDB, 12th July 2016

Kick off meetings

- July 6th Vidyo & pre GDB
- Initial meeting focused discussion
- Set initial project plan and actions
- Good participation both in person and remote - but more always welcome!

Sites

- CERN
- RAL
- CNAF
- Padova
- ECDF
- Durham
- Oxford
- Brunel
- Glasgow

Sites

- Several sites looking at what tools to use here - RAL has 2 summer students and looking at test instances

- Brunel looking at Spark (data processor) and working in wider community (co-chair CLOUDFOR16)

- Report on NCSA project to provide security appliance (*Science DMZ Actionable Intelligence Appliance*): watch with interest

- Report on status of CERN SOC

Considerations

- Importance of trust groups and relationships - new approaches
- Important to involve appropriate institutional security teams
- Complex area and diverse toolset
- SOCs are tools - benefit comes from operational use

Mandate

- 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.

Initial steps

- Initial plan is to choose particular components and build from there
- Long term and short term goals
- Awareness of sites with existing components that can be reused
  - Don’t impose solutions but work on compatibility
  - Can diverge but maintain goals

Plan & actions

- MISP Threat Intelligence sharing

Plan & actions

- MISP Threat Intelligence sharing

- Bro Network Security Monitor

Plan & actions

- MISP Threat Intelligence sharing
- Bro Network Security Monitor
- Metron Security Operations Centre

Plan & actions

- MISP Threat Intelligence sharing
  - Proposal for RAL T1 development Central instance with trust group work with NGI UK Security Team
  - ECDF/Glasgow MISP site instances
- Bro Network Security Monitor
- Metron Security Operations Centre

Plan & actions

- MISP Threat Intelligence sharing
  - Proposal for RAL T1 development Central instance with trust group work with NGI UK Security Team
  - ECDF/Glasgow MISP site instances
- Bro Network Security Monitor
  - Durham, Brunel, RAL (proposed)
- Metron Security Operations Centre

Plan & actions

- MISP Threat Intelligence sharing
  - Proposal for RAL T1 development Central instance with trust group work with NGI UK Security Team
  - ECDF/Glasgow MISP site instances
- Bro Network Security Monitor
  - Durham, Brunel, RAL (proposed)
- Metron Security Operations Centre
  - Use as reference design; general action to review structure

Next steps

- Next planned meeting in a month
- WLCG Workshop
- Participation welcome!

wlcg-soc-wg@cern.ch