SOC WG Pre GDB

Notes from previous meeting

Scope

- Single product, selection from compatible components?

- Needs of CERN/T1 different to small site with less manpower

- Start with larger sites or build up from smaller?

- Character of stakeholders (VO teams vs site/campus)

- Ingesting of VO data [CERN]

- Complex issue, what do sites have?

- Size of cluster/data/bandwidth

- Need for clarity, clear objectives

Tools & Projects

- MISP, Bro, Metron, Prometheus mentioned

- Could deploy MISP and Bro at different sites for testing

- Central MISP at CERN?

- One model vs convergence

- needs of sites with existing tools deployed

- compatible interfaces

- modularity/ flexibility

Deliverables

- WLCG Workshop

- Publications (CHEP, ACAT, CLOUDFOR16)

Agenda

- 1410: Site status/plans
- 1500: Discussion: Approach
    - Scale up or scale down, Initial test plans - suggestion of MISP & Bro, Define first steps
- 1545: Break
- 1600: Discussion: Deliverables
    - Mandate, Actions, WLCG Workshop, Publications (CHEP,ACAT,CLOUDFOR2016)
- 1645: Meeting schedule & next meeting
- 1655: AOB

Mandate

- Establish a clear set of required (data) inputs and outputs.

- Examine current and prospective SOC projects & tools.

- Create a reference design for larger sites/sites with experience with a security appliance for smaller sites/those that wish it.

Proposal

- Long-term/short-term goals & Large projects/small projects
- Suggest work on different components building from basic blocks
    - *MISP for sharing framework, Bro for data collection*
- Suggest Metron as reference design - follow & track
    - *Guide work - don't force sites with tooling to change but check interfaces for compatibility as we go*
    - *Suggest sites can diverge but maintain goals*

Proposal: work packages

- MISP at different sites -
  - local
  - central
  - API access
- Bro deployment investigation
- Metron: Initial inventory leading to working group timeline
  - Types of installation, structure…
- As we define meeting structure, plan to look at different components

CERN

- Can provide assistance with puppet modules for
  - MISP over summer
  - Bro
- Central MISP instance if needed

Publications

- WCLG workshop: status
- CLOUDFOR16: Bro developments
- ACAT: Bro + MISP