V0 and security discussion notes.

D. Petravick

US LHC Big V0s

- US LHC VOs make software choices and operate certain infrastructure.
- To obtain overall security, We need to treat the US LHC VOs perforam their this work with security in mind.
- What is required for a VO to do this? human capital, Technical tools and support apropos an organization with dynamic resources.

Some Things Static Organizations do.

- Static organizations keep an inventory of their assets.
- Static organizations have the notion of "perimeter", active defense measures.
- Static organizations are able to able to assess and measure the vulnerabliity of their as-deployed computing plant.

VO feature potential

Timescale	Security Example Feature
hours	forensics Awareness
minutes	anomaly detection security auditing fuzzy use of out of band tools
instantaneously	perimeter feedback and control

Dire scenario incident response

- One dire case is operating a vulnerable system. There would be constant work.
- As good as our ability to respond.
- The time to respond can be crucial.
- A good information system would be invaluable, since we our systems will be quite dynamic.

Accountability

- It is always good to know.
- Dp we need to provide best practices input so that our systems will be properly assessed? Is this even possible?

Proposal?

- Propose to investigate and build an information system for VO's with features apropos for security.
- Work weighted for nearly real-time system.
- To give weight for accountability.