OSG RA Status and Plans

D. Petravick

July 10, 2006

RA scope

- Current scope Is our “core”
  - The direction since Gainesville.
- What is “core”
  - It is enumerated in the Analysis overview.
  - Intent is to be what the OSG institution has clear responsibility for.
  - But
    - Is not the VO’s
    - Is not the Sites
    - Hmm on the support centers

Comments

- Since Security cannot be sprinkled on, Thinking about computer security forces thinking about the OSG as a organization.
  - We will beg deep questions about the OSG organization.
  - Have taken advantage of our proximity to Ruth.
- Don thinks we will benefit by thinking though our internal needs before thinking of the needs of VO's and sites.

Risk Analysis

- More complete
  - Brief outline of the organization
  - Methodology Section
  - Threat Section
  - Vulnerability Section
  - Impact Section
- Much Done
  - (Existing) Control Section
- To be completed
  - Residual Risk Section
  - Additional Control Section

Brief Outline of…

- Software Stack and Release Process.
- Communications and Web Presence Process
- User's Process
- Hosted VO process
- Validation, monitoring and Accounting Process
- Inter-grid operation process
- Security process.

Threats

- Careless or uninformed authorized person
- Squatter (unauthorized persons who use our resources, but not at an economically significant level)
- Vandals (web page defacers, data destroyers, malicious code, vandalize reputation)
- Thief (take services, money, things of value)
- Author who writes malware
- Spy
- Alarmist

Vulnerabilities

- Reliance on third parties for the services our processes rely on.
- Improper or inappropriate OSG core staff actions.
- Improper or inappropriate OSG user actions.
- Remote Access
- Exploits latent in vulnerable software
- Physical Access

Impact Analysis

- Draft Input -- CMS and LIGO.
- Three levels LOW MEDIUM HIGH
- LOW
- "A security event has LOW impact if it occurs less than 10 times per year and does not disrupt the perception of the OSG as a computational facility that can be relied on AND no single occurrence of the event disables the substantially all OSG's operational Compute Element service for more than two days."
- MEDIUM
  - > 20X/year disable for a week
- HIGH
  - More than this.

Technical Controls

- Configuration Management Standards for Agreements.
- Baselines (w.r.t software we require)
- Vulnerability identification (for the OSG Stack)
- Control of administrators and users.
  - E.g. QA on mailing lists, etc

Risk Mitigation and Residual risks

- Brief interviews of Doug, Leigh, Alain
- Not yet in the document.
- Additional mitigation -- (convolved controls editorial problem)

(Existing) Controls

- A defect in the document is that we have not separated existing from “things we obviously want.”
  - Template-itis, This is being worked on.
  - Is a lapse we should not make, and should not do this lest others do this to us.
  - Our intuition may not be right.

Management Controls

- Integrated security management
- Policy on core agreements

Operational Controls

- Security Process lifecycle
- Security Awareness for the Core Staff
- Security Working Group
- Security Plan Self Assessment and peer review
- Computer Security Roles and Responsibilities
- Policies and Procedures
- Information Classification
- Critical Single points of Failure Analysis

Plan

- Finish core RA
  - – Done when accepted by "Ruth".
  - – Then goes into a lifecycle hopper
- Are then in a position to consider sites and VO's
  - – But more involved, since grid interoperation is important.