ESGF Software Security Working Team (SSWT)

Prashanth Dwarakanath

NSC, Sweden

December 10, 2015

ESGF Software Security Working Team (SSWT)

- Co-leads Prashanth/Phil?
- Looking for more collaborators.
- To put out best practices guide for data node administrators.
- To identify potential risks with ESGF and provide feedback/headsup to developers, or put out a call for assistance.
- To provide assistance with post-incident data gathering/forensics preservation.
- To conduct security sessions/seminars to help bring people up to speed

Security incident review: Linköping Code Sprint

Participants: DRKZ, CMCC, LIU, PCMDI, STFC, KNMI

Issues identified

- Communication: lack of preexisting secure channels for communication.
- Communication: delay in information transfer.
- Communication: extent of severity not communicated quickly enough.
- Expectations: No clear guidelines/documented expectations from data node operators.
- Uneven security culture: access to security resources, personnel is inconsistent across organizations.

Security incident review: Linköping Code Sprint

Issues identified

- Personnel: No guidelines from ESGF about required skills for personnel.
- Software: No installation time checks outdated components/CVE checks.
- Software: Not enough modularity: need to improve distributability of roles/services.
- Security: Unpatched kernels/out-of-date packages are vulnerable to attacks.
- Security: No integrated IDS/log analyser to detect suspicious activity.
- Security: No recommended firewall policy.

Security incident review: Linköping Code Sprint

Potential solutions

- Distribute best practices document for node administrators.
- Recommend usage of firewalling and distribute template.
- Implement lightweight log scanning module to spot suspicious activity.