Security Monitoring

on behalf of Daniel Kouril

Security monitoring

- Strives to detect weaknesses that could lead to security issues
  - Weak file permissions, missing updates, …
- Improves incident response
  - Which vulnerabilities were exposed during attack, …

Security monitoring in EGI

- Integral part of EGI CSIRT activities
  - Regular monitoring of infrastructure
    - Following up critical issues
  - Certification (only sites in good shape can join the infrastructure)

- Several key services operated
  - Pakiti
  - Nagios (secmon)
  - Security dashboard

Security monitoring in Engage

- Focus on clouds
  - Wider attack surface, which sites don't entirely control
  - Sites need to address issues caused by random users (VM owners, users)

- Attacks are common and growing – not much targeted so far, though.
  - Using similar vectors – missing, weak passwords, not updated security issues
  - Getting rid of common vulnerabilities will prevent from a large number of common attacks.

Security monitoring for IaaS clouds

- Assessment of images
  - Checking they are kept updated, ...
  - Can be performed on project level (appdb), certification of images
  - Only “supported” OS/filesystems can be checked
- Monitoring of running VMs
  - Part of certification process and also best practices recommended to cloud providers
  - Detection of known vulnerabilities that often leave to compromise (password-based authentication for SSH, …)
- Network monitoring
  - Recommendations for cloud providers, image owners
  - Examination of gathering and utilization of network monitoring (e. g. netflow) for purpose of security monitoring

Activities for WP3

- Effort not available for significant development
- Focus on summarizing best practices and guides from NGIs/institutions
  - e.g. CESNET has long experience with network monitoring
- Support of project-level activities – checking of images in AppDB.
- Certification of images, ...