

CSIRT 2012 milestones

- Q1 revisit

- To address the scaling problem of Access Monitor Module by Q1 of 2012. This module tests if a certain x509-proxy can be used to access services at a site (ban-monitor)
 - Via GridFTP interface
 - Performance issue if more than 10 sites
- SSC5 regional run in NGIs, to pilot at least one NGI run in Q1 of 2012, and assist NGI security officers for their regional runs after the initial pilot
 - Find VO, attacking DNs and registration with VO, done
 - Testing job submission, problem with Pakiti
 - NGI can use their own ticket system, but SSC-RTIR is available
 - a checklist is available
 - Spanish NGI run will start on Wednesday (25th April)
- Security Dashboard further development & improvement based on gathered feedback, expect to be released in Q1 of 2012
- Migrate domain name of CSIRT Nagios box from current srv-102.afroditi.hellasgrid.gr into *.egi.eu domain (e.g. secmon.egi.eu)

CSIRT 2012 milestones

- Q2
 - CSIRT face to face meeting
 - RTIR hands-on training
 - Improving issuing handling with RTIR and any further improvement
 - To extend SSC5-framework and integrate more job-submission methods (ATLAS panda had been fully integrated), Globus, gLite job submission and VO-Job-Submissions-Frameworks (as needed) will be integrated by Q2 of 2012
 - In progress
 - Glite-ce/wms and globus-job-run/submission, done
 - The SSC6 preparation
 - VO CMS, done. attacking DN and register with CMS VO?
 - 16-27 July
 - 40 sites/20 countries, max 4 per country, only site supporting CMS VO
 - Technical
 - Integrate job submission will start Early May
 - Test open, will start ASAP
 - Need experts in CMS experiment

CSIRT 2012 milestones

- Q2
 - Pakiti (Version 3) is expected to be released in Q2 of 2012
 - Under development, should be released in Q2
 - To define and optimize security alerts (as shown in security dashboard) handling workflow, explore the possibility of integrating non-critical security operation into normal day to day operation, expect to implement an initial workflow by Q2 of 2012
 - GGUS integration
 - Procedure change require
 - Use cases
 - Alert registered in security dashboard, ticket open via GGUS, handled by sites/NGIs
 - The same as above, in addition, DC is required to provide more information, GGUS and RTIR integration
 - Ticket opened by EGI CSIRT via RTIR,
 - site-wide security monitoring (patch monitoring); To identify feasible solution, produce implementation plan and proposal by Q2 of 2012
 - Technical aspects
 - No SWAT, job wrapper and/or corn jobs
 - Poland and Czech pilot
 - Need management buy-in

CSIRT 2012 milestones

- Q3
 - Security service challenge 6
 - Site certificate procedure update
 - Security training at EGI TF 2012
 - Operation procedure for compromised certificate/CA
 - To define some basic security metrics, which are calculated through security dashboard; expecting to produce regular security metric reports (monthly or quarterly) by Q3 of 2012

CSIRT 2012 milestones

- Q4
 - Evaluation SSC6
 - nagios: CRL checking on services that have gridftp (CEs/SEs) and checking for known vulnerable file permissions via gridftp
- Ongoing activities
 - Daily operation and Incident handling
 - SSC5 NGI runs
 - Issuing handling improvement
 - Meetings
 - Identify federation, IPV6 and Cloud security

Issues to be discussed

- SSC5 NGI run
- Security training at GridKa school
- Security training at EGI TF