EGI-CSIRT Operational Security

EGI CSIRT Security Officer on Duty

Security Resource Centre Certification Procedure SEC05

EGI-Engage is co-funded by the Horizon 2020 Framework Programme
of the European Union under grant number 654142

Security Probes / (re-)Certification

Problem description

- Processing of (re-)certification requests takes very long, because ...
- EGI-CSIRT needs Security Monitoring Data from the sites to be able to apply the procedure SEC05.
- Uncertified (Suspended) Sites do not automatically get security monitoring jobs (probes)
- Currently manual intervention by Secmon people/Operations/EGI-CSIRT is needed.
- in addition, EGI-CSIRT has no means to tell if a security issue (unpatched) that led to site suspension is resolved.

Security Probes / (re-)Certification

Proposed solution

- The needed actions are easily carried out by the sites, they can run the Security Monitoring jobs manually. Install/run software is their job, we do not need Grid-Job-Submission systems for the (re-)certification purpose.
- This can be achieved by changing the procedure.

SEC05 Request for change

Old Version

	Responsible	Action	Prerequisites
1	RC	Ask the ARGO/SAM EGI Support (through GGUS http://ggus.eu/) to enable security monitoring of the site.	
2	RC	Once monitoring is enabled, RC asks EGI CSIRT (by sending a mail to csirt@rt.egi.eu) for security assessment.	Secmon team handled request from 1
3	EGI-CSIRT	If no security alert is raised via the monitoring over 3 consecutive calendar days period, the EGI CSIRT will communicate back a positive assessment.	Secmon system is working properly

SEC05 Request for change

New Version

	Responsible	Action	Prerequisites
1	RC	Follow instructions on https://wiki.egi.eu/wiki/EGI_CSIRT:Pakiti_client Install and run pakiti client on random WN. In case of re-certification on node subject to suspension.	
2	RC	check results for the RC in question https://pakiti.egi.eu/. Notify EGI-CSIRT when the problem is solved.	
3	EGI-CSIRT	EGI CSIRT verifies the results and communicate back a positive assessment, PROC09 can continue	

SEC05 Request for change

Result

- Dependencies on certification status in GOC-DB removed
- Dependencies on other Support-Units Removed (Secmon)
- No NGI Involvement
- How quick a re-certification is done depends on the RC