Security monitoring

Daniel Kouril

January 2022

Security Monitoring in EGI

- Detection of weaknesses or vulnerabilities
  - Done by CSIRT, alarms raised when necessary
  - Monitoring reactions to CSIRT advisories, alerts
- Run in parallel to other monitoring, following the same principles and tools
  - Only public interfaces utilized
- “non-intrusive” monitoring, e.g. no exploitation
  - false-positives may appear

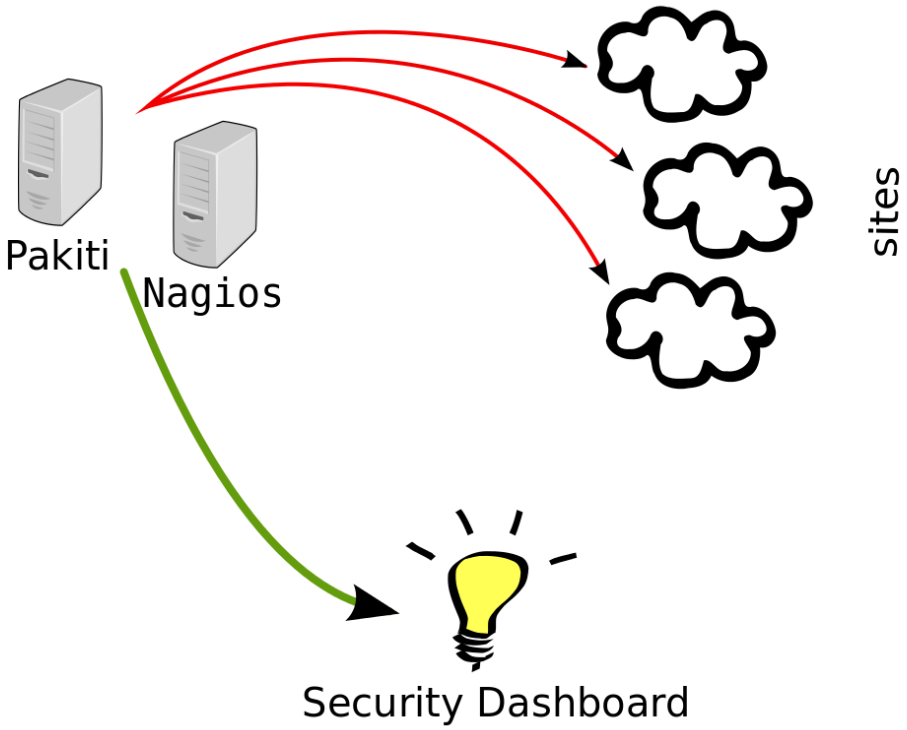
Nagios

- Service maintained by GARR
- Probes mostly by CESNET
  - https://github.com/ARGOeu/secmon-probes
- Standard EGI installation of “Nagios”
- Results consumed by Security Dashboard
- Periodic run of probes to Ces
  - Some probes are “chained” together, esp. mitigation checks

Service	Status	Last Check	Duration	Attempt	Status Information
eu.egi.sec.ARC-CE-result-ops	OK	01-13-2022 04:21:31	267d 16h 34m 32s	1/2	Job succeeded.
eu.egi.sec.ARC-CE-submit-ops	OK	01-13-2022 09:01:33	0d 6h 57m 1s	1/2	Job not finished.
eu.egi.sec.ARCCE-Pakiti-Check-ops	OK	01-13-2022 09:02:12	59d 23h 26m 31s	1/3	Pakiti-Vuln OK - magic02.farm.particle.cz: No vulnerabilities found in Pakiti.
eu.egi.sec.WN-CRL-ops	CRITICAL	01-13-2022 04:21:31	960d 13h 36m 19s	3/3	magic02.farm.particle.cz: ERROR: Some errors found. Please check details.
eu.egi.sec.WN-FilePermVulns-ops	OK	01-13-2022 04:21:31	980d 16h 36m 42s	1/3	magic02.farm.particle.cz: OK: Permissions of files with known vulnerabilities are fine
eu.egi.sec.WN-Pakiti-ops	OK	01-13-2022 04:21:31	119d 9h 16m 7s	1/3	magic02.farm.particle.cz: OK: Pakiti reported correctly to all the configured servers.
eu.egi.sec.WN-Permissions-ops	OK	01-13-2022 04:21:31	980d 16h 36m 42s	1/3	magic02.farm.particle.cz: OK: No world writtable files or folders found
eu.egi.sec.WN-RDSModuleCheck-ops	OK	01-13-2022 04:21:31	980d 16h 36m 42s	1/3	magic02.farm.particle.cz: OK: Could not open socket -- module probably blacklisted.
eu.egi.sec.WN-Torque-ops	OK	01-13-2022 04:21:31	74d 14h 55m 33s	1/3	magic02.farm.particle.cz: qmgr is not available. Assuming that other LRMS is used.
eu.egi.sec.WN-check_CVE-2013-2094-ops	OK	01-13-2022 04:21:31	980d 16h 36m 42s	1/3	magic02.farm.particle.cz: No CVE-2013-2094 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-check_CVE-2015-3245-ops	OK	01-13-2022 04:21:31	306d 14h 38m 1s	1/3	magic02.farm.particle.cz: No CVE-2015-3245 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-check_CVE-2016-5195-ops	OK	01-13-2022 04:21:31	309d 9h 36m 9s	1/3	magic02.farm.particle.cz: No CVE-2016-5195 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-check_CVE-2018-1111-ops	OK	01-13-2022 04:21:31	311d 23h 37m 47s	1/3	magic02.farm.particle.cz: No CVE-2018-1111 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-check_CVE-2018-12021-ops	OK	01-13-2022 04:21:31	309d 9h 36m 9s	1/3	magic02.farm.particle.cz: No CVE-2018-12021 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-check_CVE-2018-14634-ops	OK	01-13-2022 04:21:31	309d 9h 36m 9s	1/3	magic02.farm.particle.cz: No CVE-2018-14634 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-check_CVE-2021-3156-ops	OK	01-13-2022 04:21:31	330d 17h 36m 50s	1/3	magic02.farm.particle.cz: No CVE-2021-3156 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-check_EGI-SVG-2016-5195-ops	OK	01-13-2022 04:21:31	309d 9h 36m 9s	1/3	magic02.farm.particle.cz: No EGI-SVG-2016-5195 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-check_EGI-SVG-2018-14213-ops	OK	01-13-2022 04:21:31	309d 9h 36m 9s	1/3	magic02.farm.particle.cz: No EGI-SVG-2018-14213 vulnerability found, skipping the mitigation check
eu.egi.sec.WN-dcache-perms-ops	OK	01-13-2022 04:21:31	980d 16h 36m 42s	1/3	magic02.farm.particle.cz: No vulnerable permissions found in "/usr/share/srm/lib /usr/share/srm/conf"

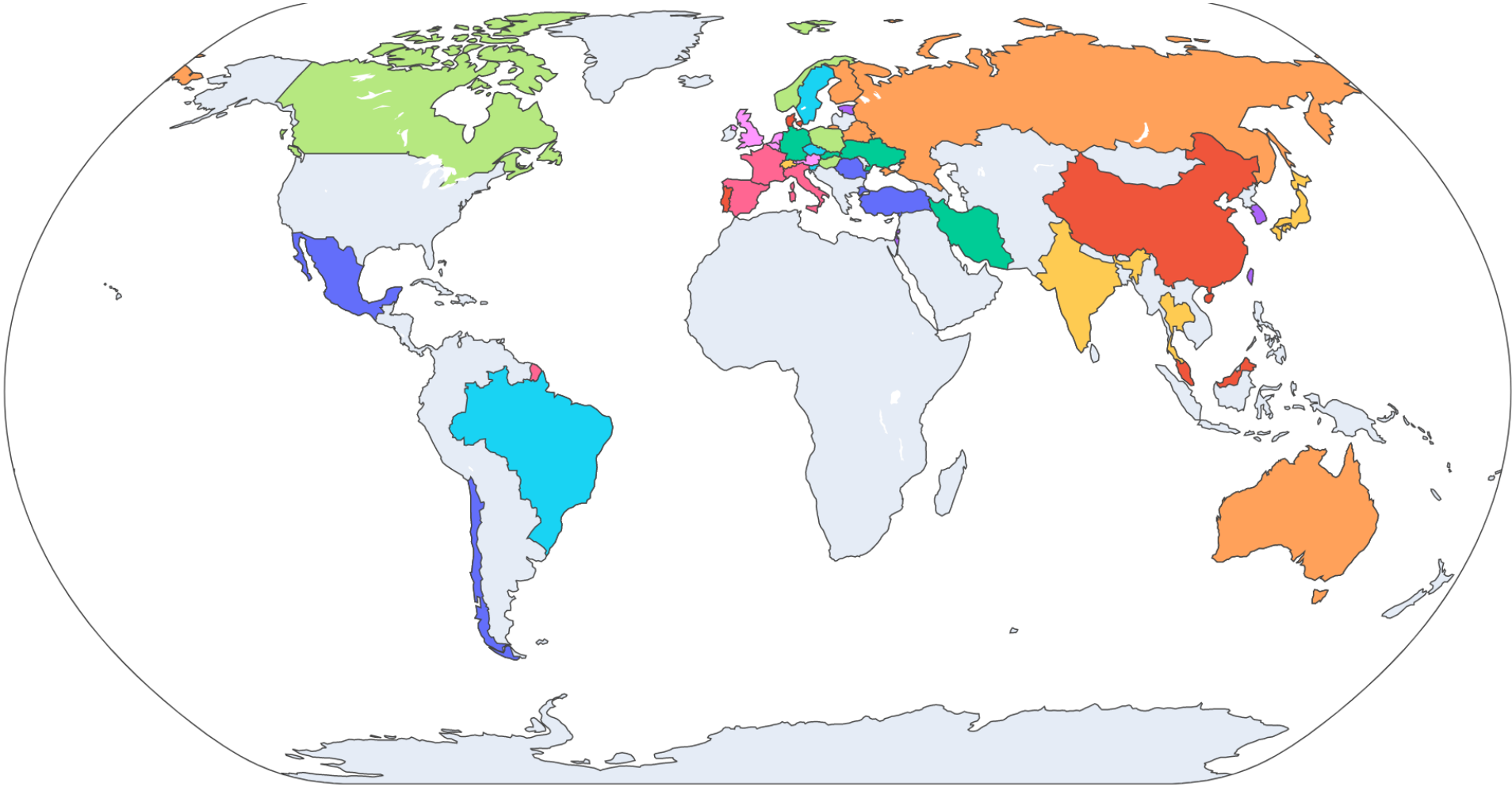
Security Dashboard

- Part of EGI Operations Portal
- Collects and stores monitoring information
  - https://secmon.egi.eu/probe_definitions.xml
- Sends notification on critical problems



Patch monitoring

- Pakiti
  - Developed and maintained by CESNET
    - https://github.com/CESNET/pakiti-server/
  - Pakiti v3
    - Better performance, easy installation, integration with EGI
- Pakiti in EGI
  - Complete switch to Pakiti v3
  - Some bugs and issues addressed lately
  - Basic log processing



https://pakiti.egi.eu/stats/

Plans

- Mainly support and maintenance
- “Monitor the monitoring”
- Addressing patches in post-CentOS era