Security Monitoring in EGEE

D. Kouřil[1], R. Brunetti[2], D. Fouossong[3], C. Kanellopoulos[4], G. Misurelli[2], M. Procházka[1], E. Ryabinkin[5], C. Triantafyllidis[4], R. Wartel[6], J. Casey[6], E. Imamagic[7] K. Skaburskas[6], S. Traylen[6], J. Shade[6], K. Pogonowski[6]

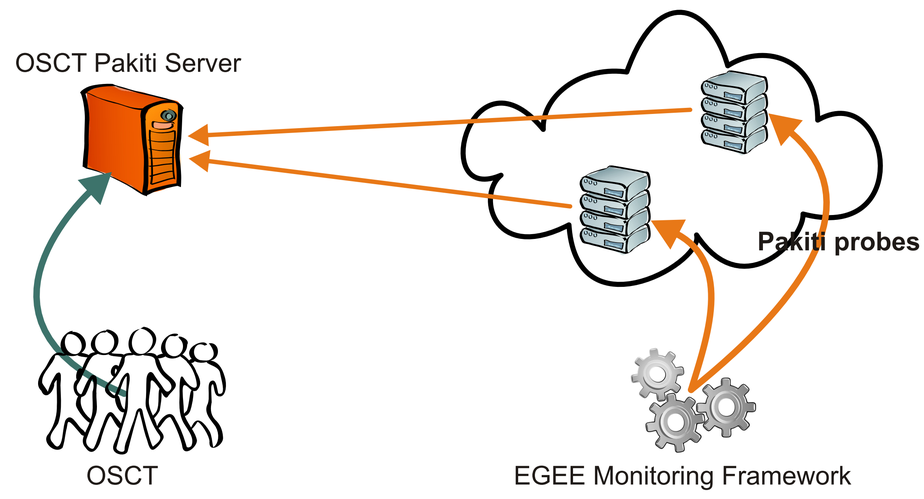
[1]CESNET, [2]INFN, [3]CNRS, [4]AUTH, [5]RRC KI, [6]CERN, [7]SRCE,

The primary goal of security monitoring, as performed by the EGEE Operational Security Coordination Team (OSCT), is to achieve and keep a high level of overall security on the project level. Security monitoring is meant to provide an overview of the situation on sites as visible from the outside. The OSCT is primarily concerned with monitoring performed from the level of the project and/or ROC. The tests only utilize the public interfaces that sites already expose and do not require any additional privileges granted by the site. Results of security monitoring are only available to authorized people.

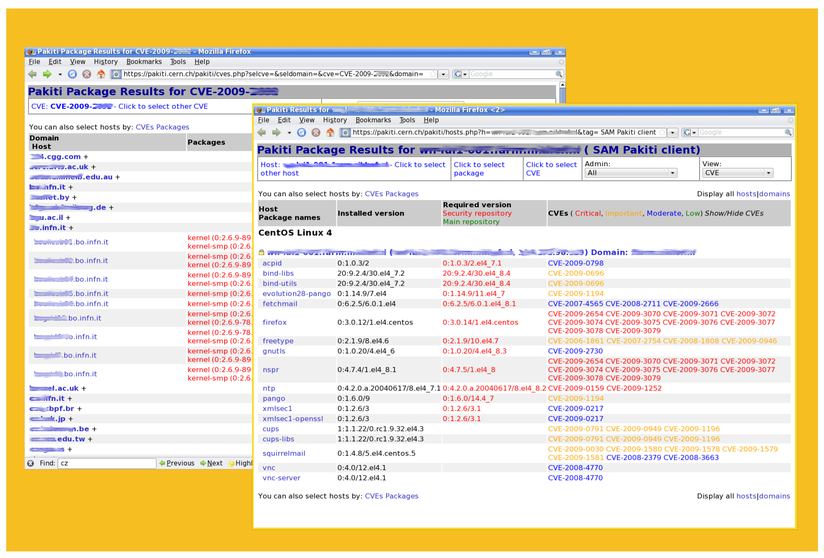
Site-level security monitoring goes beyond the scope of the OSCT and currently is deemed as minor. Currently the OSCT makes use of the SAM framework with a very basic set of probes. Further development has been primarily focused on integration of security monitoring features into the new monitoring framework based on Nagios, which is developed by the EGEE Operations Automation Team (OAT). The existing SAM security probes have been already ported to the new system and a new one (Pakiti client) developed. The OSCT and OAT groups are currently working together to define a mechanism to protect results of the probes and control access to them.

Patch monitoring using Pakiti

Pakiti [1] is an open source tool to check the patching status of monitored machines. Pakiti clients collect information about packages installed on the machine and send it to the Pakiti server. The server compares the information against the current list of updates and displays a comprehensive information about current status of all machines.
The OSCT operates a Pakiti server that is fed by Pakiti probes run as SAM or Nagios tests. If a severe vulnerability appears, the OSCT is able to identify and warn sites that need to apply security updates as has been employed recently when a critical vulnerability became public. Using the information the OSCT is able to track sites vulnerable to a specific security issue. OSCT members have been actively contributing to Pakiti development. The Pakiti architecture has been redesigned recently and a prototype implemented. Pakiti is freely available and anyone can install their own Pakiti server to monitor their machines. A Pakiti sensor is also available for Nagios, which makes it easier to integrate Pakiti with existing Nagios-based monitoring.

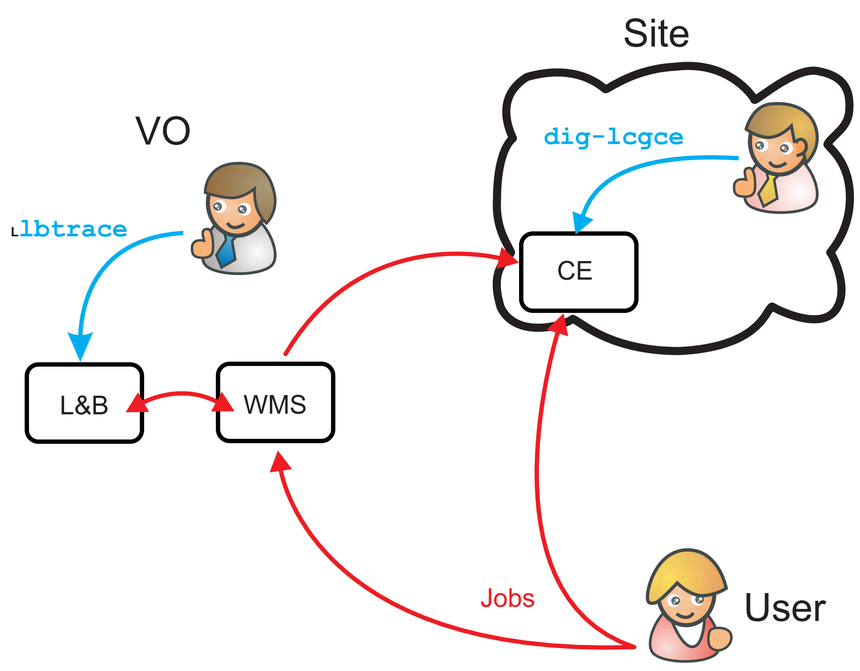


The OSCT Pakiti server monitors about 4500 hosts, of which majority is not patched. Metrics are being prepared to detect seriously vulnerable machines.



Tracing users

Acquiring information about users' activities is crucial for several areas of operational security. When a user is involved in a security incident (knowingly or not) it is important to overview the steps they did during a particular period of time to find out the domains that may be influenced by the incident. Information about users' actions performed is important not only for incident resolution but it may also contribute to reveal malicious activities done by a user (deliberately or with a stolen credential). People involved in operation security need tools and mechanisms to collect information necessary for tracing users on the grid. The OSCT is working on tools [2] that allow authorized officers to easily gather the information needed. While still under development the first version of the tools is available for usage.



VO view

The VO security officer is usually interested in having a general picture:

- What are the 10 last jobs executed on CE foo.cern.ch?
- When have been executed the 5 last jobs from DN
- Where have been executed the 10 last jobs scheduled by RB foo.cern.ch
- What executables have been run on CE foo.cern.ch since yesterday?
- When and where did we first see this DN?

Example:

```
$ lbtrace -H octopus.grid.kiae.ru list owner eq \
  '/DC=ch/DC=cern/.../CN=samoper/CN=582979/CN=Judit Novak' \
  and status eq done \
  and dst eq ce1.cern.ch:2119/jobmanager-lcgpbs-ops
```

Site view

The site administrators want to know more focused information about what was going on on the site:

- When a particular DN appeared first time on my CE?
- What DNs have been mapped to UID 1234 on the CE in the past?
- What have been the LRMS IDs assigned to a DN during the last week?

Example:

```
$ dig-lcgce -start 20090105 -end 20090107 userDN eq \
  '/C=IT/O=INFN/OU=Personal Certificate/L=CNAF/CN=giuseppe misurelli'
```

References

[1] *Pakiti project page*, http://www.sf.net/projects/pakiti/

[2] *Log analysis and tracing tools*, https://twiki.cern.ch/twiki/bin/view/LCG/LogTracing