Roadmap for transition towards EGI

Throughout its operation the OSCT has developed or identified a whole range of operational tools that are crucial for the OSCT to provide expected services. Having based on the previous experiences we put together this list of functionalities that are necessary for the OSCT and other parties involved in operational security. The OSCT has participated in a development of many tools providing the needed functionality and is going to carry on within EGEE-III. Nevertheless, many of the tools are rather pilots or even only designed and their further development will most likely be needed even after EGEE-III.

Functionality	Description, status
Security monitoring	
Integration with monitoring framework	EGEE aims at Nagios-based monitoring, to which the security monitoring should be tightly linked. In particular, security of the messaging infrastructure and access control must be addressed.
Probes for security monitoring	OSCT uses three basic security probes, it's needed to design and implement other probes, i.e. based on current risk analysis in order to allow the OSCT to spot critical risks exposed.
Monitoring of patching status	Pakiti has proven extremely useful to identify sites that expose critical vulnerabilities. Current Pakiti implementation is still a pilot, where a lot of adaptations must be added.
Tracing users	
Tracing users' activities on grid	The OSCT produced a tool demonstrating a utilization of the L&B service. The tool requires other improvements to gather information needed and to work with historic data.
Tracing users' activities on site(s)	The OSCT produced a parser of the lcgCE, which provides a basic information about users' activities. We plan to produce other versions of the tool based on BLAH and/or supporting CREAM as well.
Log management	
(Syslog best practices, filters, ...)	Some sites need assistance with setting central syslog server and defining filters based e.g. on OSCT advisories (for example to detect IP address known to originate attacks)
Integration of/with other monitoring solutions	
(Security monitoring infrastructure)	The tools mentioned and developed are often single tools whose results must be processed manually. In order to ease maintanence an infrastructure to collect and process the results and tools would be desired.
(Utilizing the ASI)	The ASI provides a complementary approach to the OSCT's way of monitoring and also provides some interesting features. The ASI should be examined in order to find a common way of performing monitoring on both grid and site levels.

-- DanielKouril - 20-Oct-2009

This topic: LCG > OSCTRoadmap
Topic revision: r2 - 2009-11-05 - DanielKouril