PROCEEDINGS OF SCIENCE

EGI Security Monitoring

Mingchao Ma[1]
Science and Technology Facilities Council - Rutherford Appleton Laboratory
F.11 R89, Didcot Oxfordshire, OX11 0QX, UK
E-mail: Mingchao.Ma@stfc.ac.uk

Daniel Kouril, Michal Prochazka
CESNET z.s.p.o., Zikova 4, 160 00 Praha 6, Czech Republic
E-mail: Daniel.Kouril@cesnet.cz, Michal.Prochazka@cesnet.cz

Cyril L'Orphelin, Olivier Lequeux, Pierre Veyre
IN2P3 / CNRS Computing Centre, Domaine scientifique de La Doua
43 bd du 11 Novembre 1918, 69622 Villeurbanne Cedex,France
E-mail: cyril.lorphelin@cc.in2p3.fr, olivier.lequeux@cc.in2p3.fr, pierre.veyre@cc.in2p3.fr

Christos Triantafyllidis, Christos Kanellopoulos, Paschalis Korosoglou
Scientific Computing Center, Aristotle University of Thessaloniki
University Campus, GR 541 24, Greece
E-mail: ctria@grid.auth.gr, skanct@grid.auth.gr,pkoro@grid.auth.gr

Abstract - This paper presents the security monitoring tools developed and operated by EGI CSIRT. Both Nagios security monitoring tool and a patching management tool - Pakiti are introduced. A newly developed security dashboard is also presented. The paper also covers how these services are deployed and operated by EGI CSIRT.

The International Symposium on Grids and Clouds (ISGC) 2012
Academia Sinica, Taipei, Taiwan
February 26 – March 2, 2012

[1] Speaker

PoS(ISGC 2012)026

1. Introduction

As we know, security is as strong as its weakest link. This is particularly true for the vast European Grid Infrastructure – a pan-European e-Infrastructure in collaboration with National Grid Initiatives (NGIs) and several European International Research Organisations (EIROs). It is vital for the infrastructure to be able to detect security weaknesses and potential security vulnerabilities as early as possible. Over the years, the EGI CSIRT (Computer Security Incident Response Team - https://wiki.egi.eu/wiki/CSIRT) has been developing security monitoring tools to monitor the infrastructure and to alert resource providers on any identified security problem. These security monitoring tools are serving as an early warning system so that a potential security issue can be detected and addressed before it becomes a more serious problem, such as a security incident.

The paper introduces current security monitoring framework that has been implemented and used by the EGI CSIRT on daily basis. The key component of the framework is a Nagios box and a set of security probes that test known issues. The probes are run as normal computing jobs submitted to the tested site so that they exploit as much as possible the standard interfaces used by common users. We use some general probes and also develop own checks based on current operations issues. We discuss the framework in more detail later in the paper.

The EGI CSIRT pays special attention to monitoring software patch status of the sites since we have learned that unpatched yet known vulnerabilities are quite often abused by attackers and lead to severe security incidents. In order to detect systems that expose critical vulnerabilities, the Pakiti [2, 3] monitoring tool has been developed and is regularly utilized by the EGI CSIRT. Pakiti was introduced at the last ISGC conference [2] so we here provide an update and describe how the service is integrated with the whole monitoring framework.

Due to the large and increasing number of resources joining the EGI e-Infrastructure it becomes more and more challenging for the EGI CSIRT to follow up all identified security issues. To solve the problem and scale up the operation capability, a security dashboard (https://operations-portal.egi.eu/csiDashboard) has been developed, which allows resource providers' security officers and their NGI operation staff to access the monitoring results, and therefore to handle the issues directly. The dashboard aggregates the data produced by different security monitoring components and provides interfaces to its visualization. Access to the collected data is subject to strict access control so that sensitive information is accessed in a controlled manner. The security dashboard was developed as a specific module of the common EGI Operations portal and we believe the handling of security issues will be incorporated with current (non-security) issue handling procedure, which will significantly reduce the overall operation cost.

The rest of this paper first introduce the Nagios-based security monitoring framework in section 2, followed by description of EGI Pakiti monitoring tool in section 3. The EGI security

dashboard is then detailed in section 4 and the conclusion and further work is presented in section 5.

2. Nagios-based Security Monitoring

2.1 Overview of Nagios Security Monitoring

Nagios (http://www.nagios.org/) is a powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes. The Security monitoring via Nagios is based on the work done by the former EGEE III OAT team and continued by the EGI JRA1 SAM team who have extended the Nagios to monitor the performance such as availability and reliability of EGI distributed computing infrastructure by using grid endpoints. This functionality allows the probing of the Grid services to be executed as a normal user job without the need of changing any configuration at the sites.

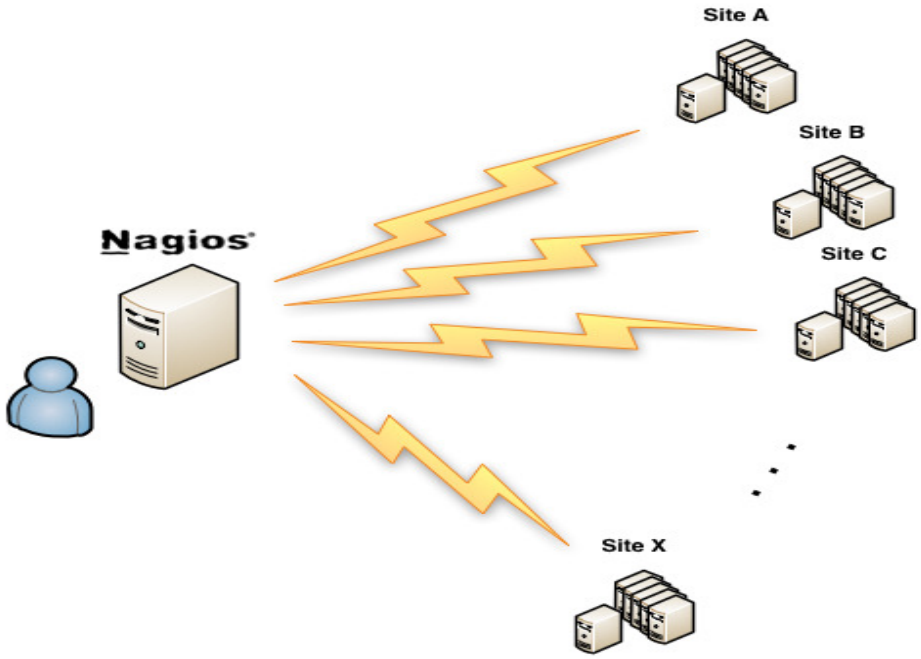

Figure 1: Nagios Security Probe Submission

Nagios is capable of monitoring hosts and services in two ways: actively and passively. The major difference between active and passive checks is that active checks are initiated and performed by Nagios, while passive checks are performed by external applications. The Nagios based security monitoring solution employed by EGI CSIRT combines both active check and passive check. The active check is used to submit normal grid jobs to the sites and the passive check is used to get the results.

As shows in Figure 1, at pre-defined regular intervals, Nagios sends a grid job to each computing element of the infrastructure with a payload of pre-defined security probes. The job

eventually lands on one of sites' worker nodes where the job executes its payload - the security probes. These security-related probes are developed and maintained by EGI CSIRT. The result of each probe is encrypted with the Nagios server host certificate, which is included in the job payload. The encrypted result is sent back to the Nagios server via the EGI Messaging infrastructure. As the result is encrypted with the Nagios host certificate, only the Nagios server can decrypt the results with its own private key. The encryption ensures the integrity and confidentiality of the monitoring result. After the decryption, the result is then imported as passive results in the Nagios service. A strict access control has been put in place so that only authorized person can access these results via the Nagios web interface. Further enhancement has now been implemented. The EGI security dashboard now can import Nagios security monitoring results and displays them via its web interface (see section 4 for detail).

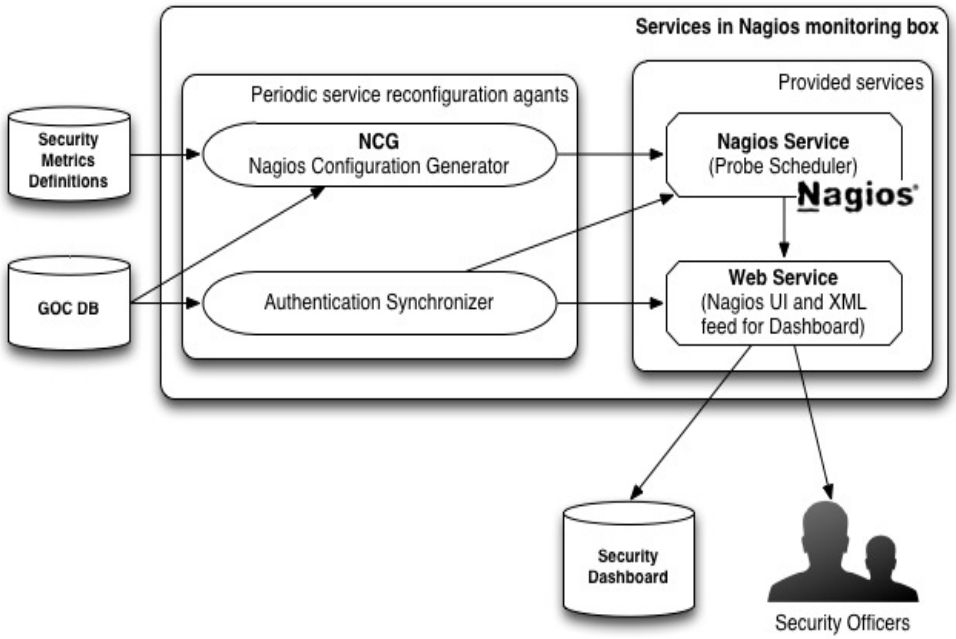

Figure 2: Architecture of Nagios Security Monitoring

Although all certified EGI sites are monitored by EGI Nagios Security Monitoring tool, only one worker node per computing element can be probed at any given time. This is due to the fact that the security probe is executed as a normal grid job. Thus only worker nodes can be checked at the moment. However, it is possible to probe other Grid services by using Grid endpoint found on Storage Element (SE) as well as Workload Management System (WMS). Development work in this area has already began.

2.2Deployment of EGI Nagio-based security monitoring

Currently there is one centralized EGI Nagios security monitoring instance deployed. The architecture of the Nagios security monitoring is shown in Figure 2. The Nagios server obtains resource centre information via EGI central database - GOCDB (https://goc.egi.eu/portal/). A number of probes developed by EGI CSIRT are currently being used to monitor the EGI. These probes are:

- eu.egi.sec.WN-CRL: this probe verifies that all CRLs exist and are current. An error message is returned if at least one outdated or missing CRL is detected while a warning message means that a CRL is about to expire.
- eu.egi.sec.WN-Permissions: this probe tries to detect world-writable files or directories in exposed environment. An arbitrary world writable file or directory could be a security risk. An error message returned by the probe means that an unexpected world writable file or directory within user's environment is detected.
- eu.egi.sec.WN-FilePermVulns: this probe tries to identify a file with wrong file permission which can be explored to escalate privilege (such as CVE-2009-4033). An error message means that a vulnerability has been found and it is exploitable while a warning indicates that a wrong file permission is detected but due to other control in place it is unlikely to be exploited.
- eu.egi.sec.WN-Pakiti: the probe reports a list of installed packages to the EGI Pakiti servers. Please refer section 3 for details of EGI Pakiti
- eu.egi.sec.WN-RDSModuleCheck: the probe checks whether the vulnerable RDS module can be loaded into memory
- eu.egi.sec.WN-Torque: Checks whether torque server that the worker node is using has vulnerable options turned on, as per EGI security advisories.

As we can see from the above list. Some security probes are general purposes probe while others are developed to detect a specific known vulnerability. The current Nagios-based security monitoring allows us to quickly deploy a new security probe to detect a newly disclosed security vulnerability.

3.EGI Pakiti

Software flaws (bugs) are almost inherently present in every piece of software. Software flaws might be explored by an attacker to reduce a system's information assurance such as to gain unauthorized access to confidential information or to escalate privilege. These software flaws are called vulnerabilities. Since software vulnerabilities can pose significant risk on computing infrastructure responsible software vendors usually address software vulnerability promptly by releasing software update or patch that fixes the problem. As the number of vulnerabilities grew, their management become more and more complex. In order to make it easier for all the parties to work with the information about vulnerabilities, the system for Common Vulnerabilities and Exposures (CVE) has been introduced. In the system every single known vulnerability is assigned a unique identifier, which can be used as the reference whenever the vulnerability is discussed. The directory of CVEs is publicly available from MITRE [4].

To help manage large number of software vulnerabilities, some software vendors, notable operating system vendors, also publish additional information that can be used to track known vulnerabilities based on the CVEs and corresponding fix or patch. In order to provide an

interoperable mechanism to express these information the Open Vulnerability and Assessment Language (OVAL) has been defined and standardized [5]. OVAL is used by many software vendors, including Microsoft, Oracle, Cisco, RedHat, SuSE.

Our operation experience has shown that security vulnerabilities are very often used by attackers to obtain unauthorized access to the systems and therefore pose a significant risk to our computing infrastructure. Thus, it is essential that all resource providers in the EGI update their systems with latest security fixes as soon as possible. However, the experience gathered over several years of operations in the EGI and its predecessors clearly shows that ensuring a homogeneous level of security across multiple, often heterogeneous, resources is challenging. This is especially the case when applying software updates, which require technical expertise and significant coordination efforts, in many cases service downtime is inevitable. Unfortunately, failure to promptly apply security updates remains one of the main causes of security incidents affecting EGI's computing infrastructure.

In order to gain visibility of security patching status across EGI, the Pakiti monitoring system has been developed.

3.1 Pakiti Architecture

Pakiti is a client/server solution with the server collecting information about installed software packages that is reported by the clients running on particular nodes of the infrastructure. The server evaluates the information and make the results of the evaluation available for further check

Pakiti is primarily focused on the Linux environment. The Pakiti client is a simple script that uses common commands to collect a list of RPM and/or DEB packages installed on the system. The Pakiti client does not require root privilege to be executed. Apart from the list of installed software package, Pakiti client also collects some additional information such as the version of the running Linux kernel and name of the Linux distribution etc. The Pakiti server is a central services which collects information reported by the Pakiti clients.

The Pakiti server consists of several modules controlling all the process, a module that retrieves input data from the clients, a processing module and a module to visualise the results. The server regularly updates its internal database with information of known vulnerabilities. These known vulnerabilities might be published by the software vendors in the OVAL compatible format which can be processed by Pakiti server. The Pakiti server can process data directly pulled from software vendors' package repositories as well.

The Pakiti server allows its operators to tag a particular CVE number with a custom flag, therefore to quickly identify any vulnerability associated with one or a group of CVEs. The information collected by the Pakiti server can be accessed via a web interface subject to strict access control. The server can also publish a machine-readable records that can be imported and

processed by other authorized services. For example, EGI Security Dashboard imports Pakiti result from the Pakiti server and present it via its dashboard interface. Since information collected by the Pakiti is sensitive, access to Pakiti result is subject to proper access control so that only authorized people could view the information.

3.2Pakiti Deployment in EGI

The Pakiti has been used in the European grids for many years and is used by the EGI CSIRT on daily basis. Whenever a vulnerability is assessed as crucial by the EGI CSIRT, it is marked as either Critical or High, based on the result of the risk assessment. These sites who are running the vulnerable software will be notified and asked to apply the updates. Failure to apply some critical security updates might lead to site suspension as per the critical vulnerabilities handling procedure [1].

Every day the EGI Pakiti server receives more than 2300 reports from EGI production sites. Authorized staff such as members of EGI CSIRT, site and NGI security officers can check the result through a web interface. A alerting email will also be sent to EGI CSIRT if a critical vulnerability has been detected. In addition to the production Pakiti server, a second backend Pakiti server is also setup to collect and store historical data. At the time of writing the second Pakiti server has collected about 400,000 reports from 22,000 nodes of 335 production sites over 6 months period.

Currently the Pakiti client is sent to sites as a payload of Nagios security monitoring job, thus there is no need to install it locally or change the configuration at sites. The output of the Pakiti client is reported to the Pakiti server via the Nagios monitoring framework, which in turn exports the result to the security dashboard, which will be discussed at following section.

4. EGI Security Dashboard

4.1 Overview of the Security Dashboard

As described previously the EGI CSIRT operates several monitoring services to collect various information from the sites and provide an overview of the infrastructure in terms of operational security and currently two services are in production: the EGI security Nagios instance and Pakiti server.

Each of these monitoring services implements respective access control and provide their own web interfaces to access results. Clearly this is not ideal. The goal of the EGI security dashboard is to aggregate data produced by the current EGI security monitoring tools, to process these data and provide a single coherent interface for accessing the result. The dashboard should be extensible so that additional source of information can be integrated when needed. A proper access control should be put in place so that security information will be accessed at a need to know basis.

4.2 Architecture

To ensure flexibility and performances of the security dashboard, a three-tier model was developed. The architecture of the security dashboard is depicted in figure 3. The three-tier model was originally developed for the Central Operations Dashboard (http://operations-portal.egi.eu/):

- Web interface
- Data aggregation & unification service called Lavoisier (http://grid.in2p3.fr/lavoisier)
- A MySQL database.

The Lavoisier service is developed at CC-IN2P3, France and is used in the development of EGI Central Operational Portals. The core function of Lavoisier service is to store, consolidate data from various sources and export data in a consistent format to the web interface. It can also cache information from various sources therefore increase the resilience of the overall system from intermittent unavailability of information sources. It is designed to enable easy and efficient cross-data sources queries. All information is presented in XML format and XSL is used to query these data sources.

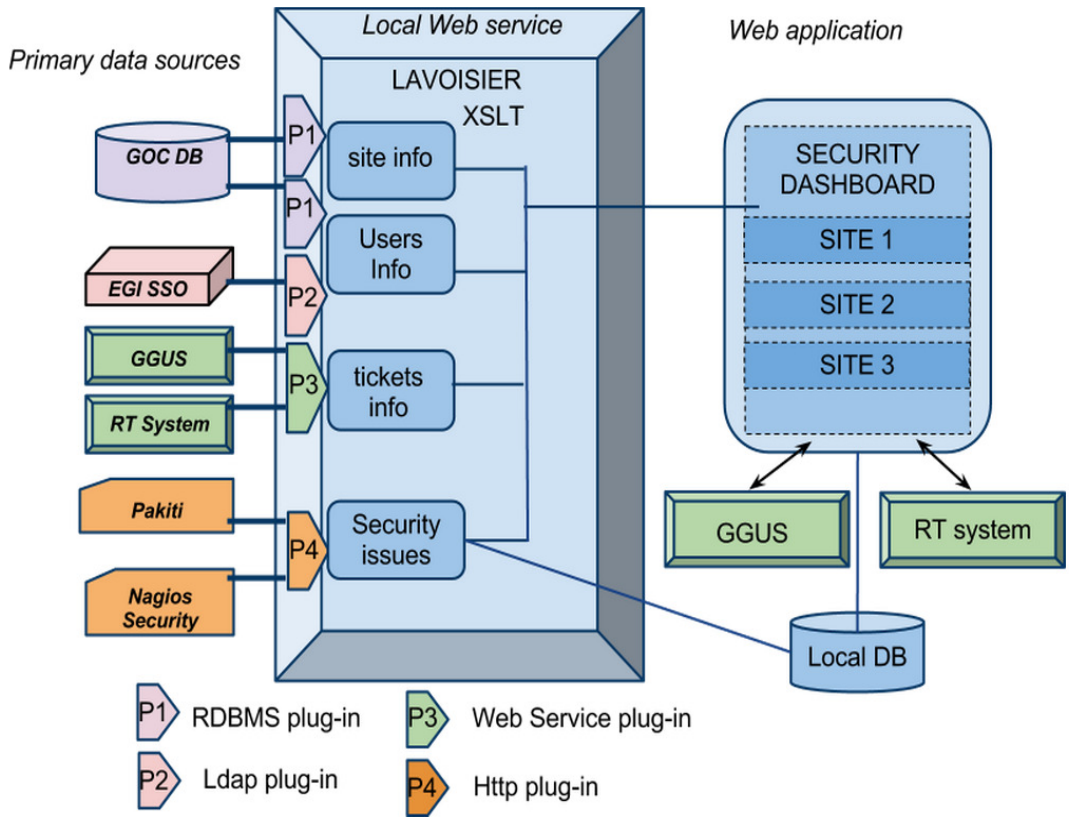

Figure 3: Architecture of Security Dashboard

To interact different data sources, the Lavoisier service employs the concept of plug-in or adapters. Each data source has a dedicated plug-in to interact with Lavoisier service. The output of the plug-in is in XML format. Currently Lavoisier is able to connect to following data sources via different programming interface:

- GOCDB: for site information, security contacts information and security roles
- GGUS/RT: for all information related to tickets
- EGI SSO: for information of EGI CSIRT members
- Nagios and Pakiti: for all security-related information

As showed in Figure 3, the plug-in acts as an abstract layer to hide the difference of data source from the upper layer components. The abstract will allow additional data source to be added without any change of the existing components.

4.3Advanced Feature

To protect security dashboard from unauthorized access, a role-based access control model is implemented. The permission to access the content of the security dashboard is based on the role associated to the certificate of the user. These roles information are defined in GOCDB and EGI SSO. Following roles are defined and used for access control by the security dashboard:

- Members of EGI CSIRT who will have full access to the security dashboard without any restriction
- NGI security officer or a NGI operator will be able to access all sites information within his/her own NGI. They can't access other NGI sites information
- A site security officer or a site administrator will be able to access information about his/her own site only

By logging on the security dashboard web interface, an authorized user with a proper role will be able to :

- Access to security alarms reported by Pakiti and Nagios
- Send a notepad to a given site
- Access all messages exchanged with the site's operator
- Open a ticket via GGUS / EGI Helpdesk to a given site linking on-going alarms
- Access and update tickets opened via the dashboard

The security dashboard also provides a web interface to visualize the monitoring results in different format. It allows operators to dynamically display the security monitoring result either in a table or in a chart format which can be customised via following options:

- the range of date
- the scope of the monitoring result such as a site or a NGI
- the type of result such as Nagios result or Pakiti result
- the format of the visualization, either depicted as a table or a chart

The security dashboard also allows an authorised user to define and declare an event, which can then be shared with other authorised operators. This will assist the collaboration of dashboard operators.

4.4 Deployment

The EGI security dashboard is now in production. It is co-hosted with EGI operational dashboard and can be accessed with a web browser. Now site administrators and NGI operation staff have a single place to check normal operational issues as well as security alerts. Both site and NGI security officers are now able to access security alerts concerning his/her sites or NGIs via a standard web interface. It also allows the NGI operation staff to follow up with a site in question on any outstanding security issues. Before the security dashboard was released, it was very difficult to engage the NGI operation staff and NGI management to follow up any particular security issue concerning his/her site or NGI, as they were not able to access such information.

To optimise the use of security dashboard and streamline issue handling procedure, a proper issue handling workflow and escalation procedure is being developed. The workflow will allow security officer, site administrators, NGI operation staffs as well as EGI CSIRT to work together to solve any security issue detected by the security monitoring tools. The aim of the procedure is to ensure that most non-critical security issue will be handled locally by the site and/or by NGI without the need of escalating to EGI level, which will free up effort and time from EGI CSIRT so that they can focus their efforts on more critical security problem such as security incident or a critical vulnerability.

5.Limitation, Further Work and Conclusion

5.1 Limitation

As discussed in section 2, the basic principle employed in the EGI security monitoring model (Nagios) is that no special access to the sites is required. The security probes are injected as normal computation jobs which will be executed under the identity of a normal user. The drawback of this approach is that the security probe can only run on one work node at site at any given time. For various reasons the security probe more than often lands on the same set of worker nodes, which makes it impossible for the CSIRT to get information about all the nodes exposed by the site, which means it is impossible to have a comprehensive picture of site security posture. Surprisingly some sites installations are not homogeneous in terms of packages or even operating systems installed on the cluster nodes. In order to gather a comprehensive picture about the installed packages and their status we are looking into ways of how to obtain information from every node of a site. There are several possible technical mechanisms that are being considered such as execution Pakiti client via a cron job, utilization of the SWAT framework, extending the VO submission frameworks, adapting the jobwraper scripts, or their combination.

5.2 Further Work

The results of the security monitoring will be used to improve site security as well as the whole EGI. We will utilize the Security Dashboard to raise security across EGI sites. Further enhancement on the security dashboard will continue. According to the monitoring result, a series of security metrics are being defined. In the near future both NGI management and EGI management will be able to access site and NGI security metrics report similar to current site availability and reliability report.

5.3 Conclusion

Our current experience has shown that security monitoring has played a vital role when dealing with security threat. It is almost impossible to carry out any meaningful risk assessment without knowing some basic information about sites and NGIs. Being able to detect a known security vulnerability allows us to quickly mitigate the risk by alerting sites in question. Many sites are also glad to have the monitoring tool in place to tell them what is going on at their sites so that action can be taken before a security threat might be materialised.

References

[1] EGI-CSIRT Critical Vulnerability Operational Procedure, https://documents.egi.eu/document/283

[2] M. Prochazka, D. Kouril, R. Wartel, C. Kanellopoulos, C. Triantafyllidis, *A Race for Security: Identifying Vulnerabilities on 50 000 Hosts Faster than Attackers*, in Proceedings of Science (PoS), 2011 International Symposium on Grids and Clouds (ISGC 2011), Taipei, Taiwan, March 2011.

[3] Pakiti, *A Patching Status Monitoring Tool*, http://pakiti.sourceforge.net/

[4] The MITRE Corporation, *CVE – Common Vulnerabilities and Exposures (CVE)*, http://cve.mitre.org/.

[5] The OVAL language, *Open Vulnerability and Assessment Language*, http://oval.mitre.org/