EGI DASHBOARD SECURITY
FUNCTIONAL SPECIFICATIONS

**1. Access control**

**Overview**

Security Dashboard will be in full HTTPS and specific credentials could be applied for each feature and component. ROD/COD/Site Administrator will not have any credential for the first release of security dashboard; indeed actions through security dashboard
are not yet properly defined for these roles. CSIRT members and related roles will be retrieved from LDAP server, Security Officers from GOCDB.

**Actions/Questions**

 - Confirm credentials for following features: view/note/metrics (see ‘*Credentials by feature’*)

 - Complete credentials for: report/tickets features (see ‘*Credentials by feature’*)

 - Shifting:

 => Is there a shift system?

 => Do you want to manage it with an handover tool or something else?

**Credentials by feature**

* **view**

|  |  |
| --- | --- |
| EGI view  | global view of security dashboard : all NGIs, all Sites |
| NGI view  | global view of a given NGI and related sites |
| SITE view  | single site view |
| Role | EGI view | NGI view | SITE view |
| EGI CSIRT members | true | True | true |
| NGI Security Officer | false | true if owner | true if owner |
| Site Security Officer | false | False | true if owner |
| Site Administrator | false | False | true if owner |
| ROD | false | true if owner | true if owner |
| COD | true | true | true |

* **ticket against site : RT ticket managment**

|  |  |  |
| --- | --- | --- |
| Role | View | /update/close |
| EGI CSIRT members | True | true |
| NGI Security Officer | True if owner | True if owner |
| Site Security Officer | true if owner | false |
| Site Administrator | True if owner | false |
| ROD | True if owner | True if owner |
| COD | true | true |

* **site reports access**

|  |  |
| --- | --- |
| Role | view |
| EGI CSIRT members | true |
| NGI Security Officer | true if owner |
| Site Security Officer | true if owner |
| Site Administrator | true if owner |
| ROD | true if owner |
| COD | true |

* **site note : tool to add a note related to site issues**

|  |  |  |
| --- | --- | --- |
| Role | view | submit/delete |
| EGI CSIRT members | true | true |
| NGI Security Officer | true if owner | true if owner |
| Site Security Officer | true if owner | true if owner |
| Site Administrator | true if owner | true if owner |
| ROD | true if owner | true if owner |
| COD | true | true |

* **metrics**
-----------

|  |  |
| --- | --- |
| Role | view |
| EGI CSIRT members | true |
| NGI Security Officer | true if owner |
| Site Security Officer | true if owner |
| Site Administrator | true if owner |
| ROD | true if owner |
| COD | true |

* handhover : **see questions**

|  |  |  |
| --- | --- | --- |
| Role | view | submit/delete |
| EGI CSIRT members |  |  |
| NGI Security Officer |  |  |
| Site Security Officer |  |  |
| Site Administrator | false | false |
| ROD | false | false |
| COD | false | false |

**2. Collecting security issues**

Site names in Nagios Probe feed have been added by Christos, many thanks to him.

**Actions/Questions**

 - Confirm status/label mapping for Nagios Probe

**Nagios probe : m**apping of statuses

|  |  |
| --- | --- |
| test status | label mapping |
| 0 | ok |
| 1 | warning |
| 2 | error |
| 3 | critical |

**3. Security metrics, reporting functions**

“We will start with a simple integraton of the results of Pakiti and Nagios to the existing dashboard.
 Both these services will provide an XML-based reports that will be retrieved by the dashboard on regular basis.
The results will contain the site name (as per GOC DB) and information gathered to the site."\*
....
"Define/adapt/implement/ the XML (CSV,...) format of the reports for Nagios and Pakiti and make them available for Dashboard."

**Actions/Questions**

 - Could you precise what is the difference between metrics and report ?

**4. Filtering data**

**Actions/Questions**

Is there an official list of:

* All possible CVEs
* All possible Nagios probes

We might need it to generate drop down lists for the filtering system in web pages

**5. Proposition of a web interface model**

