Table of Contents

Security Service Challenge level 3 (SSC_3)

This WIKI contains instructions, recommendations and suggestions that are relevant for the LCG/EGEE Security Service Challenge level 3 (SSC_3).

The objective

The goal of the LCG/EGEE Security Service Challenge (SSC), is to investigate whether sufficient information is available to be able conduct an audit trace as part of an incident response, and to ensure that appropriate communications channels are available.

SSC_3 challenges the Operational Diligence of the LCG/EGEE Grid Sites.

Material for the Test OPerator (TOP)

We have provided a tool kit containing software and detailed instructions for executing the SSC_3. When the SSC_3 enters the second Stage (see below), then the material will be available for download here. The ReadMe gives a little more detail about the material.

Choosing a suitable Distinguished Name (DN)

The target Site may have put restrictions on which Virtual Organizations (VO) are authorized to submit jobs. Also, they may have put additional restrictions on the characteristics of the jobs. Hence, it is necessary to identify a VO which is authorized to submit jobs that are authorized to run for at least 72 wall-clock-hours. Then TOP must negotiate with the chosen VO management in order to choose a suitable DN under which auspices the challenge will run. TOP must be allowed to gain the identity of the chosen DN.

Launch of alert

Once the challenge has been successfully launched, TOP sends an alert to the Security Contact of the Site as registered in the GOCDB. The contents of the alert is outlined below:

```
This e-mail is an alert about a TEST incident. It is executed under
the supervision of EGEE/LCG Operational Security Coordination Team
(OSCT) as part of the OSCT Security Services Challenge (SSC). More
information about the SSC can be found at

         http://cern.ch/osct/ssc.html

You are asked to following the normal incident procedure, but you
MUST_NOT take any collective action against the VO of the offending
user.

       Consider any activity from the following user as malicious.
       The distinguished name (DN) of the user is:

/DC=yz/DC=universe/OU=Organic Units/OU=Users/CN=jobu/CN=12345678/CN=John Bull

       Please handle this test incident according to the normal
       incident response procedure with the two exceptions listed
       below:

       1. No sanctions must be applied against the Virtual
          Organization (VO) that was used to submit the job.
```

```
2. All "multi-destination" alerts must be addressed to
   the e-mail list which has been designated for the test:

        project-egee-security-challenge@cern.ch

   DO NOT use:
        project-lcg-security-csirts@cern.ch
   for Security Service Challenges. Instead, insert the
   originally intended "multi-destination" address(es) in
   the body of your message.
```

Follow-up

TOP will receive copies of the e-mail exchanges that ensue. He/she makes time stamped records of the events and ensures that actions taken on the submitted job have the intended effect. The out-of band logs are used for this. Inconsistencies are noted.

Report

After completion of the challenge, a report is filed with OSCT for debriefing.

Links to related information

An initial SSC_3 was executed during the first half of 2008. The targets were a selection of LCG Tier-1 Sites.

- SSC_3_evaluationForm_v2.04.xls: Evaluation of the 2008 Tier-1 SSC_3 Security Service Challenge

Evaluations

- Evaluations

Updates:
2008-12-11 (psa) Included link to the 2008 Tier-1 SSC_3
2008-08-20 (psa) complete revision of text
2007-08-17 (psa) initial writing

This topic: LCG > SSC3
Topic revision: r10 - 2009-02-19 - PalAnderssen