Retour du regional Security Challenge

Dorine Fouossong

Atelier Sécurité Grille du 28 janvier 2010, Villeurbanne

Plan

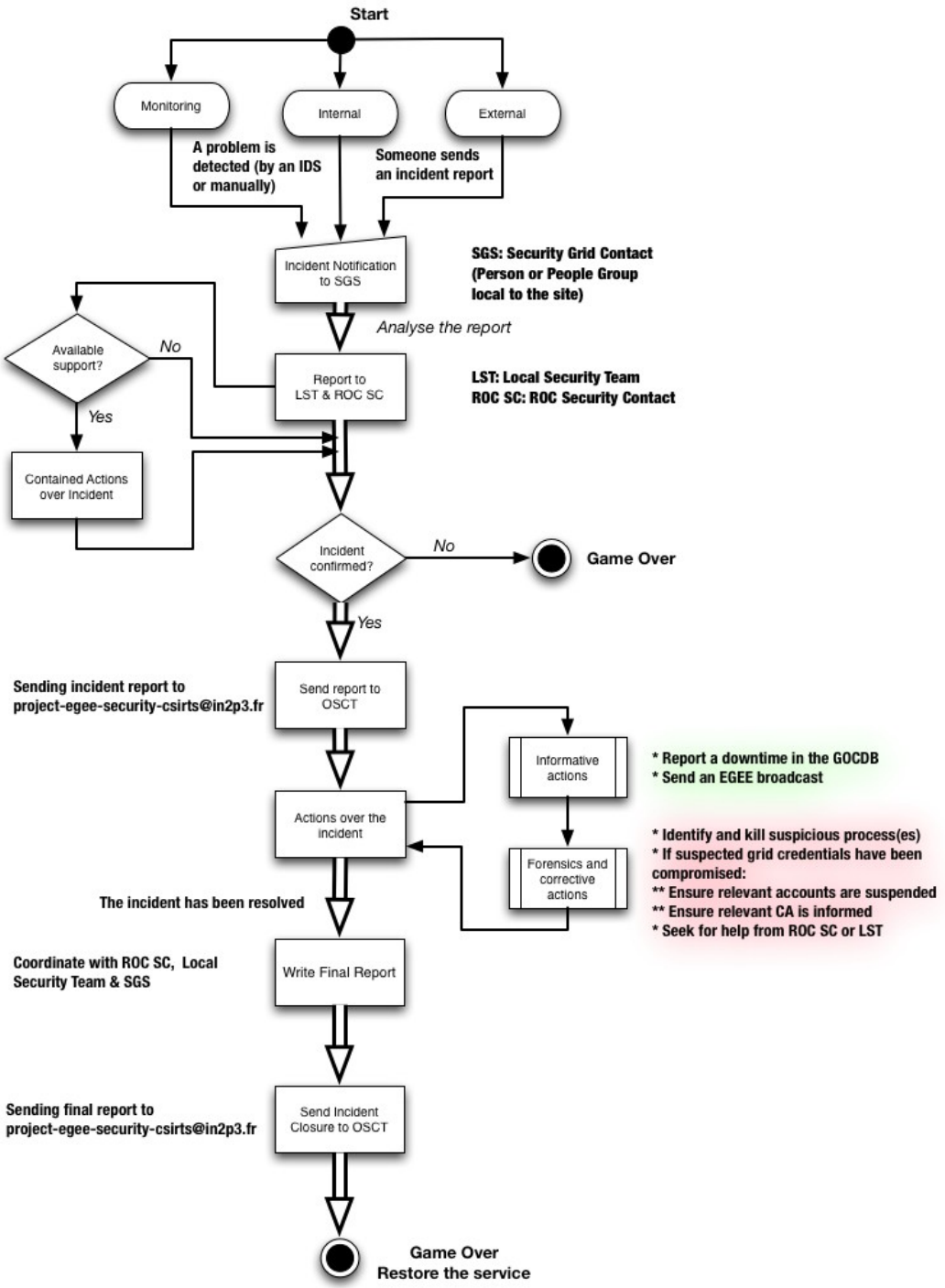
- Présentation du régional SS3
- Evaluation pour le ROC France
- Perspectives

Le premier challenge lancé à l'échelle régionale.

Objectif:

Evaluer la capacité des équipes à mener la réaction à un incident, communication sur l'incident et l'analyse forensic.

Procédure


Start
Monitoring
Internal
External
A problem is detected (by an IDS or manually)
Someone sends an incident report
Incident Notification to SGS
SGS: Security Grid Contact (Person or People Group local to the site)
Analyse the report
Available support?
No
Yes
Report to LST & ROC SC
LST: Local Security Team
ROC SC: ROC Security Contact
Contained Actions over Incident
Incident confirmed?
No
Game Over
Yes
Sending incident report to project-egee-security-csirts@in2p3.fr
Send report to OSCT
Informative actions
* Report a downtime in the GOCDB
* Send an EGEE broadcast
Actions over the incident
Forensics and corrective actions
* Identify and kill suspicious process(es)
* If suspected grid credentials have been compromised:
** Ensure relevant accounts are suspended
** Ensure relevant CA is informed
* Seek for help from ROC SC or LST
The incident has been resolved
Coordinate with ROC SC, Local Security Team & SGS
Write Final Report
Sending final report to project-egee-security-csirts@in2p3.fr
Send Incident Closure to OSCT
Game Over
Restore the service

Remarque avant de commencer

C'était une première fois.

L'exercice

Consider any activity from the following user as malicious.

The distinguished name (DN) of the user is: /O=GRID-FR/C=FR/O=CNRS/OU=LPC/CN=Dorine Fouossong Test

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

Bien communiquer

TYPE DE MESSAGE:

- En interne:

Vérifier si il y'a lieu de lancer la procédure EGEE.

- Dans le cadre de la procédure EGEE:

Rapport initial

Evolution des investigations

Cloture de l'incident

TYPE MESSAGE :

- Contact VO
- Contact CA
- Contact utilisateur concerné
- Contact csirt de la ressource à partir de laquelle le job a été envoyé, si pas de retour rapide bloquer la ressource.

L'objectif est de bannir l'utilisateur.

DESTINATAIRE DES MESSAGES

- équipe sécurité locale
- équipe sécurité ROC
- équipe de sécurité sites voisins
- sécurité EGEE

La communication avec EGEE est formelle et controlée par le correspondant incident.

Bien communiquer

Mails signés

Réactivité des équipes

Bonne structuration des rapports (hote compromis, IP suspectes, informations sur le code malveillant , actions prises).

Containment et forensics

- Maitriser le risque de propagation de l'incident
- Verifier l'éventualité d'une compromission root
- Analyse du traffic de l'UI
- Récupération de l'input sandbox
- Analyse du logiciel malicieux (analyse de code, test dans une sandbox, utilisation de logiciels de forensic libres).

Quelle évaluation faire de ce challenge?

Questions

- Comment avez vous banni l'utilisateur de vos ressources? En utilisant un outil spécifique ou alors à la main?

- Avez vous un outil de détection d'intrusion ?

Perspectives

?