ATELIER SECURITE GRILLE

SESSION INTERNE

17 novembre 2010

Dorine Fouossong
dorine.fouossong(at)clermont.in2p3.fr

- Etude de cas SSC4
- Procédure de gestion des incidents sécurité grille
- Canaux de communication et répartition des tâches
- Sécurité au jour le jour, répartition des tâches
- Besoins en service centraux

Etude de cas SSC4

Le challenge sécurité SSC4

Les challenges de sécurité permettent de vérifier que:

- **les informations utiles pour mener à bien une investigation en cas d'incident de sécurité sont disponibles et suffisantes.**
- **Les canaux de communication sont disponibles et fonctionnent de manière appropriée.**

Une alerte est soumise au site testé en l'invitant à suivre la procédure normale de gestion des incidents à l'exception près du canal de communication utilisé et de l'impact réel des décisions de suspension prises.

Pour des raisons d'évaluation, l'équipe opératrice du challenge est mise en copie de toutes les communications effectuées avec l'extérieur.

Le challenge de sécurité SSC4

Les spécificités du SSC4:

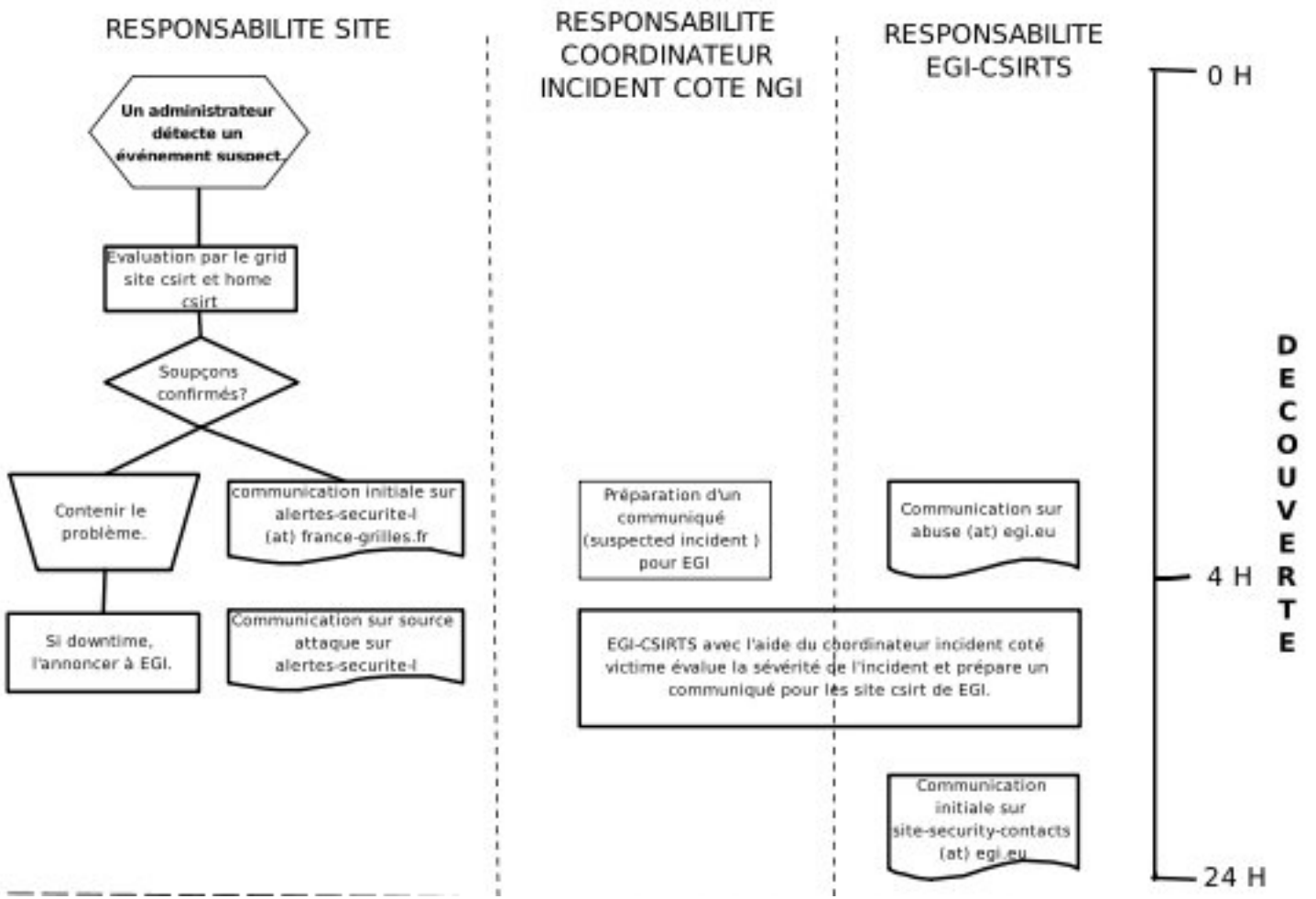
- **L'exercice utilise une plateforme de soumission de job pilot Atlas. Donc l'équipe doit communiquer avec cette VO afin de récupérer toutes les informations utiles à l'investigation. Tout en minisant l'impact de l'incident sur la VO.**
- **Lors de l'alerte initiale 2 adresses IP sont communiquées comme base de départ des investigations.**

Etude de cas SSC4

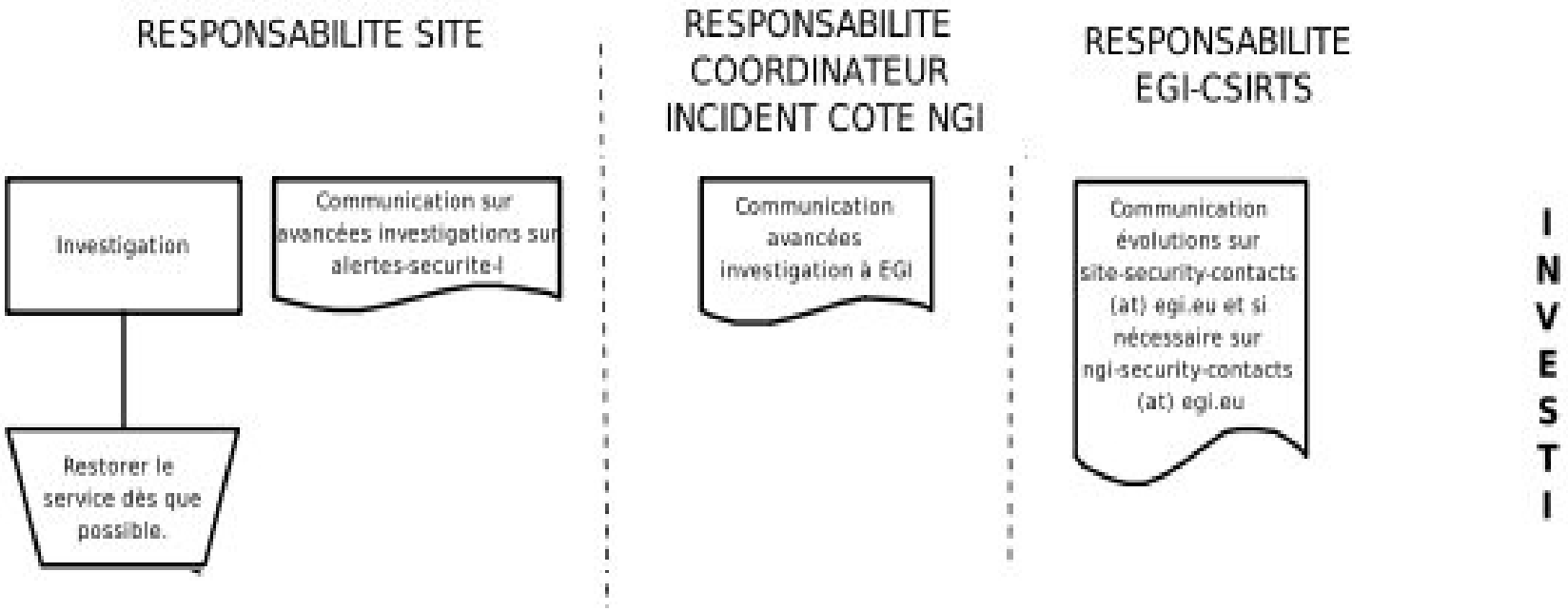
- **Le cas du centre de calcul IN2P3**

- **Procédure de gestion des incidents sécurité grille**

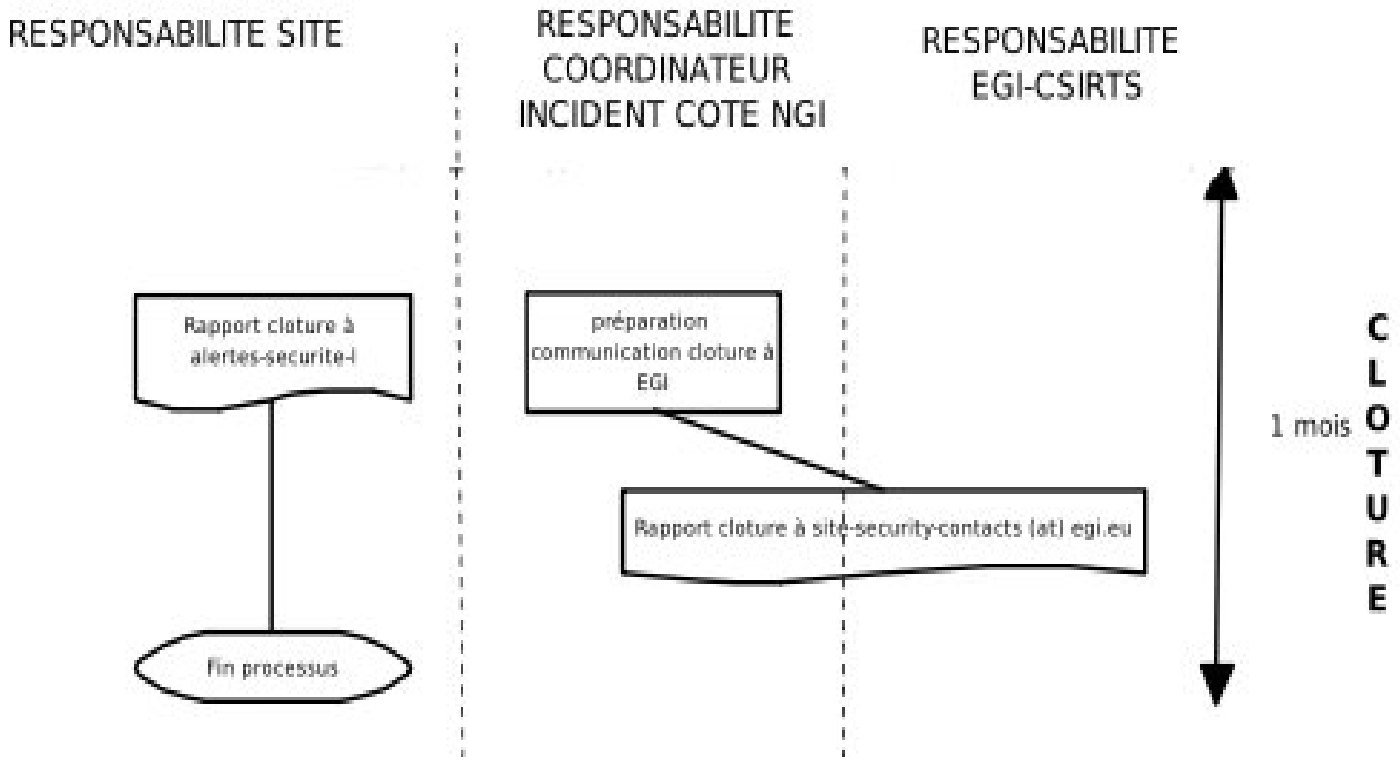
La procédure de gestion des incidents sécurité grille



La procédure de gestion des incidents sécurité grille



La procédure de gestion des incidents sécurité grille



Exercices de sécurité testant la maitrise et l'adéquation de la procédure

La prochaine étape est une campagne challenge SSC4 régional:

- **Elle concerne les T2 et sera lancée en février/mars prochain.**
- **Le framework du challenge va être adapté par rapport à celui utilisé our les T1. Il intégrera un outil de communication intégrant les templates de communication et facilitant le suivi du déroulement de la procédure.**
- **Les critères d'évaluation changeront un peu car on ne peut exiger les mêmes efforts que ceux demandés pour un T1. Le site pourra s'appuyer sur l'équipe support pour l'analyse des binaires ou du traffic réseau.**

Exercices de sécurité testant la maitrise et l'adéquation de la procédure

L'étape suivante est un big-challenge EGI:

- **Le job malveillant est déployé sur plusieurs sites.**
- **Un seul site (T2 ou T3) recevra l'alerte initiale.**

- **Canaux de communication et répartition des tâches**

Récapitulatif des canaux de communication

Canaux utilisés dans le cadre de la gestion des incidents

- **Pour envoyer de l'information:**

  alerte-securite-l(at)france-grilles.fr

- **Pour recevoir de l'information:**

  alerte-securite-l(at)france-grilles.fr

  site-security-contacts(at)mailman.egi.eu

Canaux utilisés pour les discussions

operation-securite-l(at)france-grilles.fr

Les listes de gestion des incidents

- **Il s'agit des listes alerte-securite-l et site-security-contacts .**
- **La liste des membres est synchronisée avec la GOCDB. Elle contient le contenu du champ « csirtemail » des fiches de sites en production.**
- **Les informations qui circulent sur ces listes sont sauf mention contraire réservées aux seuls destinataires.**
- **!! Les listes de diffusion référencées par csirtemail ne doivent contenir que des personnes ayant besoin d'en savoir.**

Utilisation de l'information site security officer de la GOCDB

- **Cette information est différente du contact csirt utilisé dans les canaux de gestion des incidents.**
- **Elle est de plus en plus utilisée pour donner accès à des services centraux EGI. Le DN de l'officier sécurité du site est automatiquement rajouté aux ACLs.**
- **Il est fortement conseillé aux sites de remplir ce champ.**

La liste de discussion operation-securite-l

Pour faciliter les échanges, le groupe est limité à un ou deux correspondants pour chaque site. Les macro-sites comme le GRIF sont un cas à part, un correspondant au moins par sous-site.

Le correspondant est l'intermédiaire entre le groupe opérations sécurité France Grilles et le site : faciliter la mise en oeuvre de la politique de sécurité. Pour celà il est appelé à :

- **Participer activement aux discussions et échange d'expérience**
- **Faire des rapports sur l'état de la sécurité du site**
- **Participer aux exercices de sécurité**
- **Participer aux réunions et ateliers sécurité grille**

Les correspondants sécurité de la NGI France

Les personnes qui sont impliquées dans la coordination des opérations de la sécurité de la NGI et les activités sécurité EGI sont:

Thierry Mouthuy

Frédéric Schaer

Pierrick Micout

Dorine Fouossong

<ngi-france-security-contact-l@FRANCE-GRILLES.FR>

Un ingénieur recruté auprès du LIMOS de Clermont-Ferrand nous assistera dans les développements.

Les correspondants sécurité EGI

- La liste abuse(at)egi.eu contient les membres de EGI-CSIRT impliqués dans l'activité IRTF (Incident Response Task Force) de ce groupe.
- Ces personnes ont la qualité de officier sécurité NGI et/ou membre du Security Vulnerability Group.
- L'activité IRTF est coordonnée par Leif Nixon.
- Le groupe EGI-CSIRT est coordonné par Mingchao Ma.
- L'émetteur des requêtes en cas de procédure de gestion des incidents est le « coordonateur incident coté EGI ». Il s'agit le plus souvent du contact IRTF on duty.
- Les autres messages envoyés sur la liste site-security-contacts proviennent du contact IRTF on duty.

- **Sécurité au jour le jour, répartition des tâches**

La sécurité au jour le jour

Les sites sont sollicités plus souvent que dans le passé par EGI ou la NGI, notamment, pour des mises à jour urgentes.

- **Quels enseignements tirer de l'expérience des derniers incidents?**

Besoin en services centraux

Besoins en service centraux

Les fonctionnalités dont vous avez besoin sont:

- **Bannir facilement un utilisateur**
- **Détecter les rootkits**
- **Accéder aux informations de monitoring dont dispose EGI-CSIRT**
- **Faciliter la configurations de Quattor**
- **Faciliter le suivi de l'évolution des incidents**
- **Collaborer dans la gestion de documents**

Discussion libre

MERCI DE VOTRE PARTICIPATION

N'oubliez pas notre prochain rendez-vous, le 26 novembre 10h00.

Nous parlerons entre autres de site internet et de formation sécurité grilles.