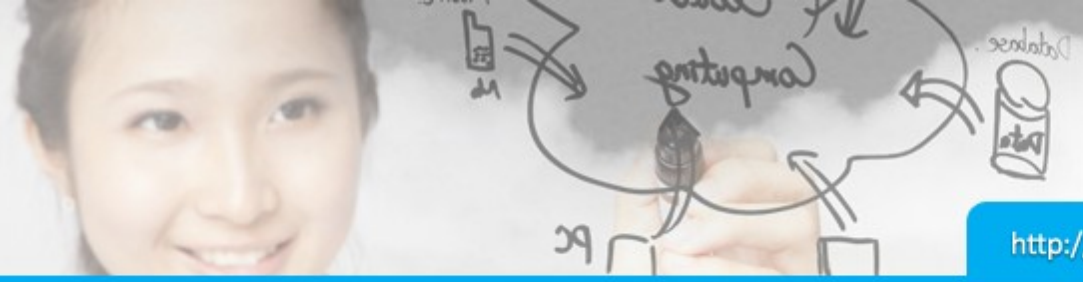
La sécurité dans le Cloud

Jérôme PANSANEL

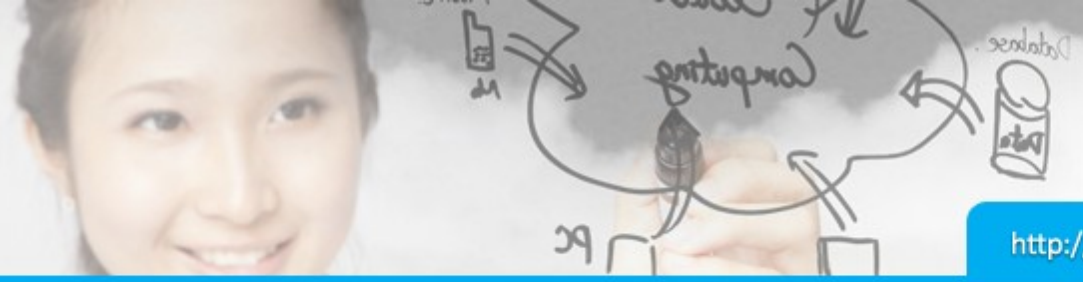
jerome.pansanel@iphc.cnrs.fr

Formation Utilisateur FG-Cloud – Avril 2016 – Lyon



Règle n°1

L'utilisateur est responsable de sa VM !



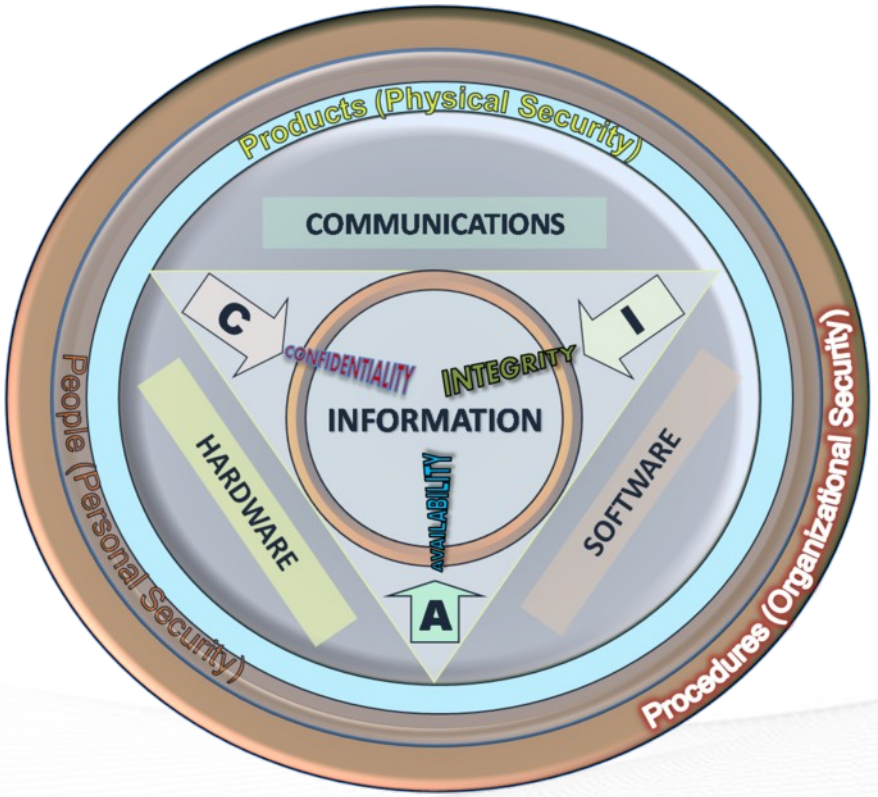
Sommaire

- Sécurité et Cloud
- Déployer un environnement sûr
- En cas d'incident

Sécurité et Cloud

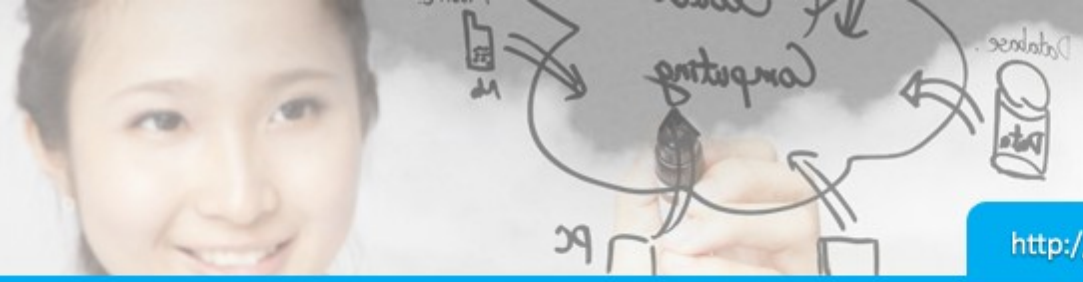
Points clés (modèle de CIA) :

- Confidentialité
- Intégrité
- Disponibilité
- *Traçabilité*



Périmètre :

- L'infrastructure
- Les procédures
- La communication vers les utilisateurs



Sécurité et Cloud

Cloud privé :

- Opéré pour une seule organisation (exemple : hébergement de services)
- Faible cloisonnement (interaction avec d'autres services du labo)
- Utilisateurs connus
- Action de sensibilisation plus facile
- Intégré plus simplement dans la PSSI de l'organisation

Cloud publique :

- Opéré pour un ensemble d'utilisateurs / organisations
- Ouvert sur l'extérieur
- La communication vers les utilisateurs peut être compliquée
- Réputation du fournisseur de ressource
- Impact sur les autres activités du laboratoire

Étude de la sécurité

- Quelles sont les procédures pour maintenir les services opérationnels et à jour, en particulier concernant les patchs de sécurité ?
- Est-ce que les différents réseaux sont séparés ? Quels sont les outils utilisés pour surveiller l'activité du (des) réseau(s) ?
- Êtes-vous en contact avec les responsables sécurité ? Sont-ils au courant qu'une infrastructure de type Cloud est déployée ?
- Comment sont sauvegardés les logs ? Sont-ils stockés de manière à ce qu'ils ne soient pas modifiables en cas de compromission ?
- Qui peut accéder au VMs ? Comment est géré cet accès ?
- Est-ce que les VMs fonctionnent sur du matériel dédié ?
- Pouvez-vous simplement suspendre un utilisateur / groupe ?

Étude de la sécurité

- Est-ce que différents rôles sont définis dans vos tenants ?
- Comment sont installées les images virtuelles ? Est-ce qu'une procédure d'endossement existe ?
- Est-ce que vous avez une procédure pour surveiller le réseau des VMs (en particulier savoir où est-ce que ce se connecte chaque VM) ?
- Les VMs d'un tenant sont-elles disponible depuis d'autres tenants ?
- Si l'utilisateur peut se connecter en tant que 'root' sur la VM, est-ce que ses connexions sont surveillées ?
- Savez-vous réaliser des snapshots ?
- Est-ce que les conditions d'utilisation de votre Cloud sont disponibles pour tous les utilisateurs ?
- Combien de temps garder vous les informations (utilisateurs, …) ?

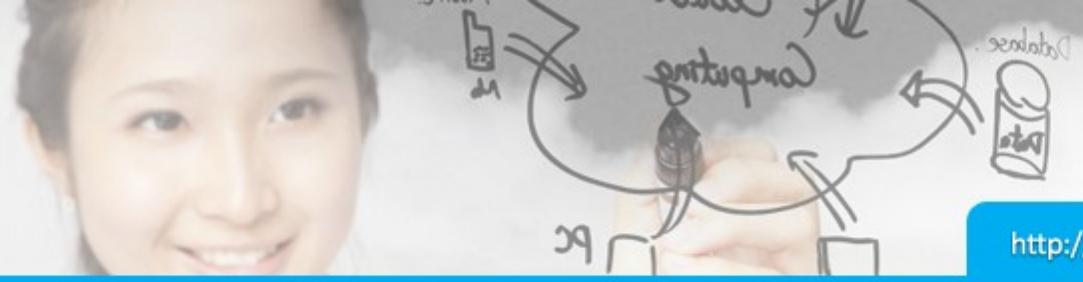
Où sont les vulnérabilités ?

Machines virtuelles

OpenStack

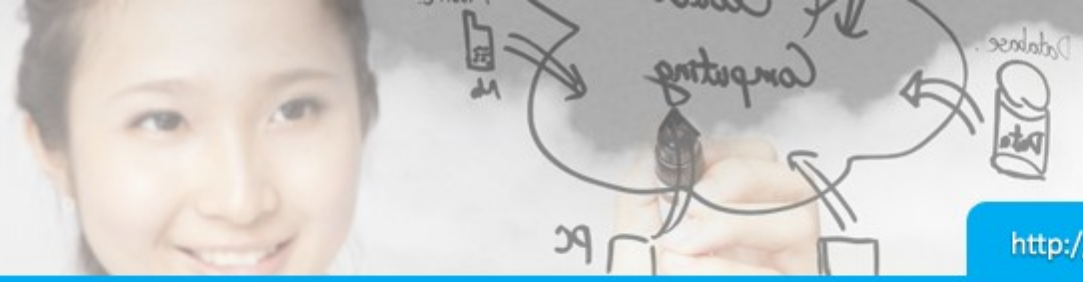
Keystone | Glance | Cinder | Nova | Neutron

OS
(http, ssh, mysql, libvirt, ...)



Sommaire

- Sécurité et Cloud
- Déployer un environnement sûr
- En cas d'incident



Bonnes pratiques

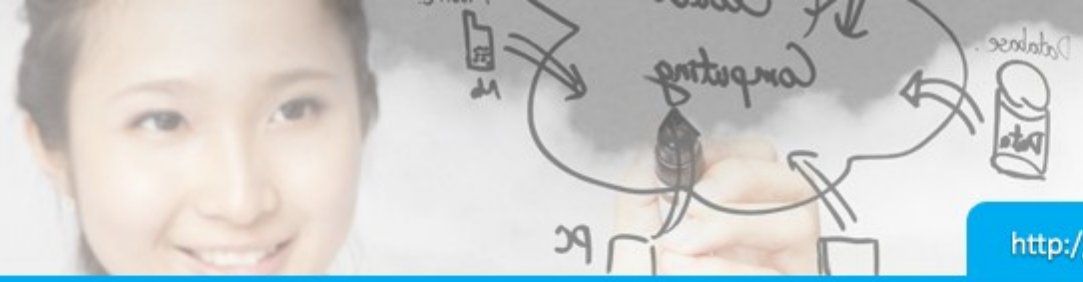
Pour éviter de faciliter la compromission de ses VMs :

- Interdire l'authentification par mot de passe (uniquement clé SSH)
- Mettre à jour régulièrement les systèmes
- Installer le minimum de logiciels
- Chiffrer les flux de données et les espaces de stockage
- Gérer finement les droits d'accès

Points organisationnels :

- Veille active des exploits de sécurité dans le domaine
- Connaître la procédure de déclaration et de réponse d'incident
- Centraliser les logs (rsyslog, ...)
- Test et surveillance des VMs (Nagios, ...)

Réf. : Guidebook on National Cyber Security Strategies (ENISA)



Bonnes pratiques

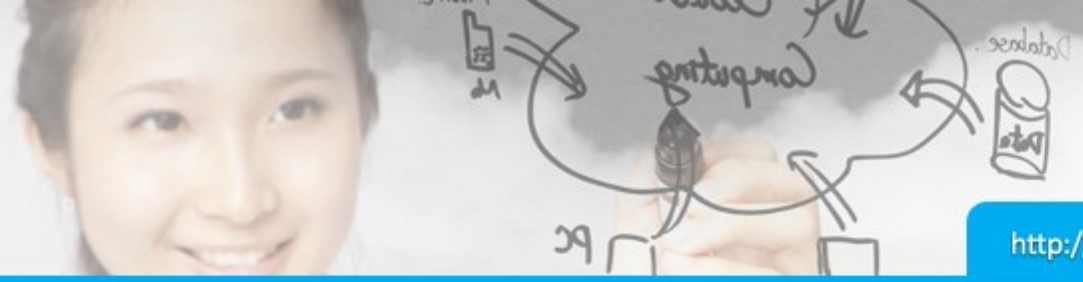
Un administrateur de VMs doit :

- Connaître ses machines
- Les analyser régulièrement
- Les éteindre si elles ne sont plus nécessaires
- Documenter les modifications
- Centraliser les configurations
- Organiser la sauvegarde des logs
- Ne pas stocker des informations confidentielles

Machines virtuelles

- Activer les mises à jour automatiques
- Bonne pratique de sécurité

  → http://iase.disa.mil/stigs/Pages/index.aspx
- Fail2Ban
- Endossement des VMs
- http://docs.openstack.org/image-guide/
- Responsabilité des utilisateurs (conditions d'utilisation)
- ...



Sommaire

- Sécurité et Cloud
- Déployer un environnement sûr
- En cas d'incident

Procédure de réponse à un incident

- Avertir le correspondant sécurité du site
- Contenir l'incident (p. e. snapshot / couper le réseau)

  → il faut garder des traces pour les étapes suivantes !
- Confirmer l'incident
- Avertir les utilisateurs de la suspension du service
- Analyse de l'incident
- Debriefing
- Remise en opération

Réf. : `https://wiki.egi.eu/w/images/f/f5/Site_Checklist.pdf`

Qui contacter en cas d'incident

Au niveau local :

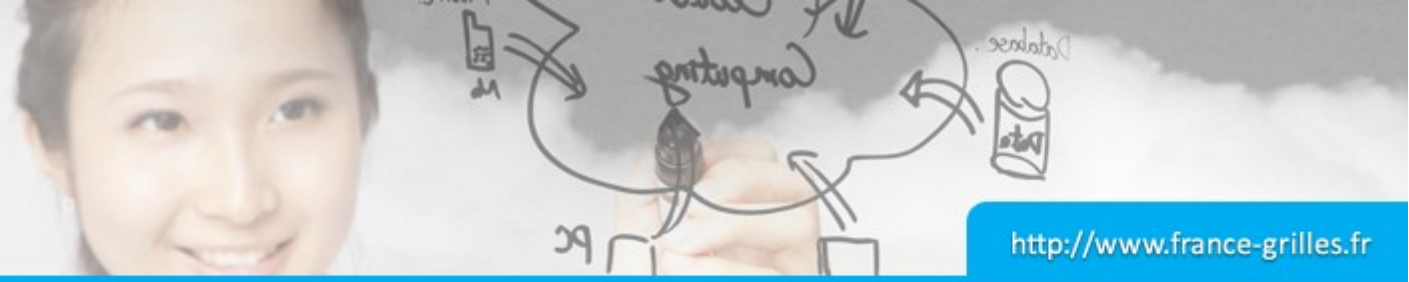
- Avertir l'équipe d'administration du site

Au niveau français :

- Sophie Ferry (France Grilles)
- → ngi-france-security-contact-l@france-grilles.fr

Au niveau européen :

- CSIRT EGI
- → https://wiki.egi.eu/wiki/EGI_CSIRT:Main_Page
- → https://wiki.egi.eu/wiki/EGI_CSIRT:Incident_reporting
- → abuse 'at' egi.eu



Questions ?