ITSR43 - Ingénierie des systèmes d'information

Partie Organisation d'un SI

Benoît DARTIES

Remontée d'incidents

Des incidents arrivent tout le temps sur un SI :

- Machines en panne
- Logiciels non mis à jour
- Bugs logiciels
- Anomalies matérielles
- « Disparition » de matériel
- problèmes mystères
- et bien d'autres …

Remontée d'incidents

Qui constate ces incidents ?

- Utilisateurs en premier lieu
- Clients du produit
- Administrateur (parfois)

Problème de la remontée d'incidents

- Comment remonter l'incident
- A qui le remonter ?

Remontée d'incidents

Facteurs complexifiant le problème

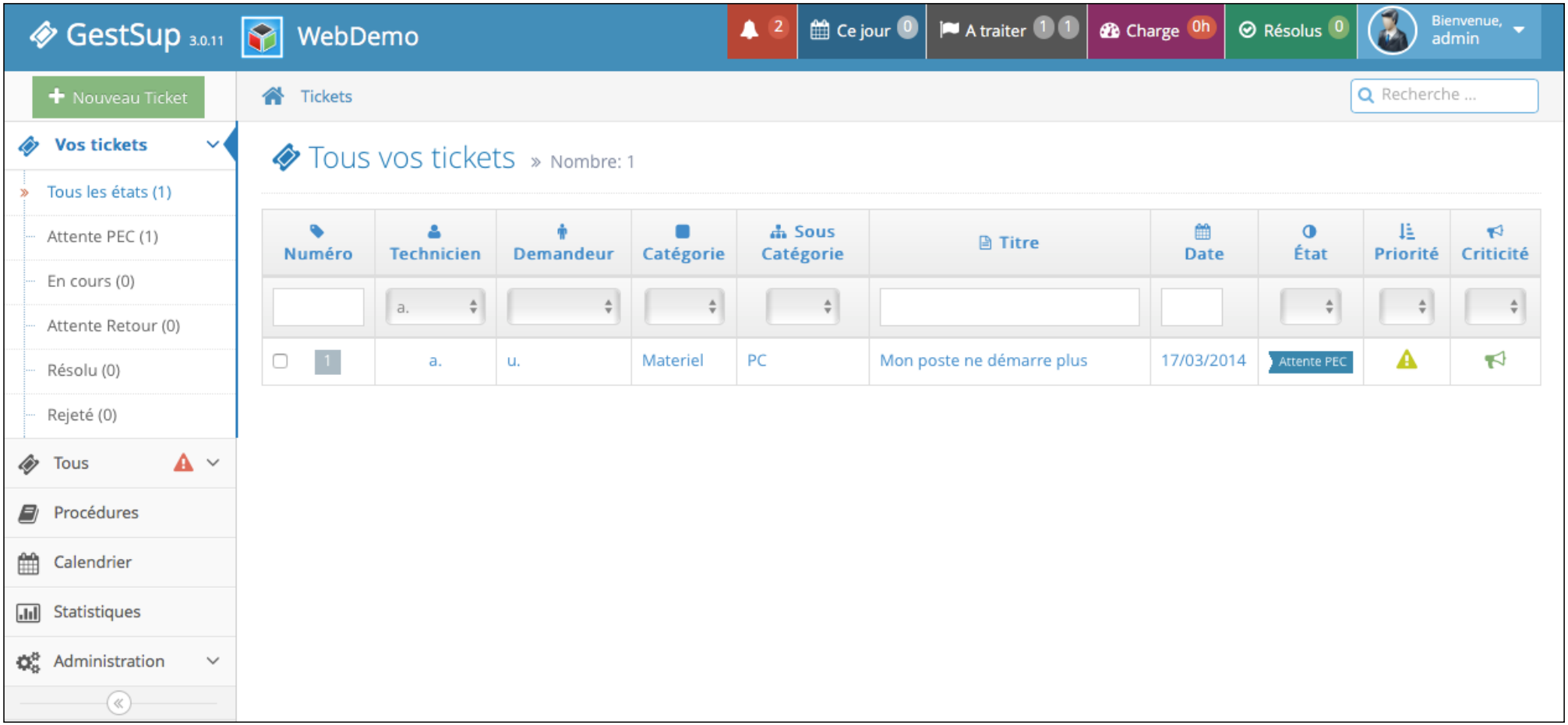
- Problèmes très divers
- Criticité des problèmes
- Plusieurs administrateurs

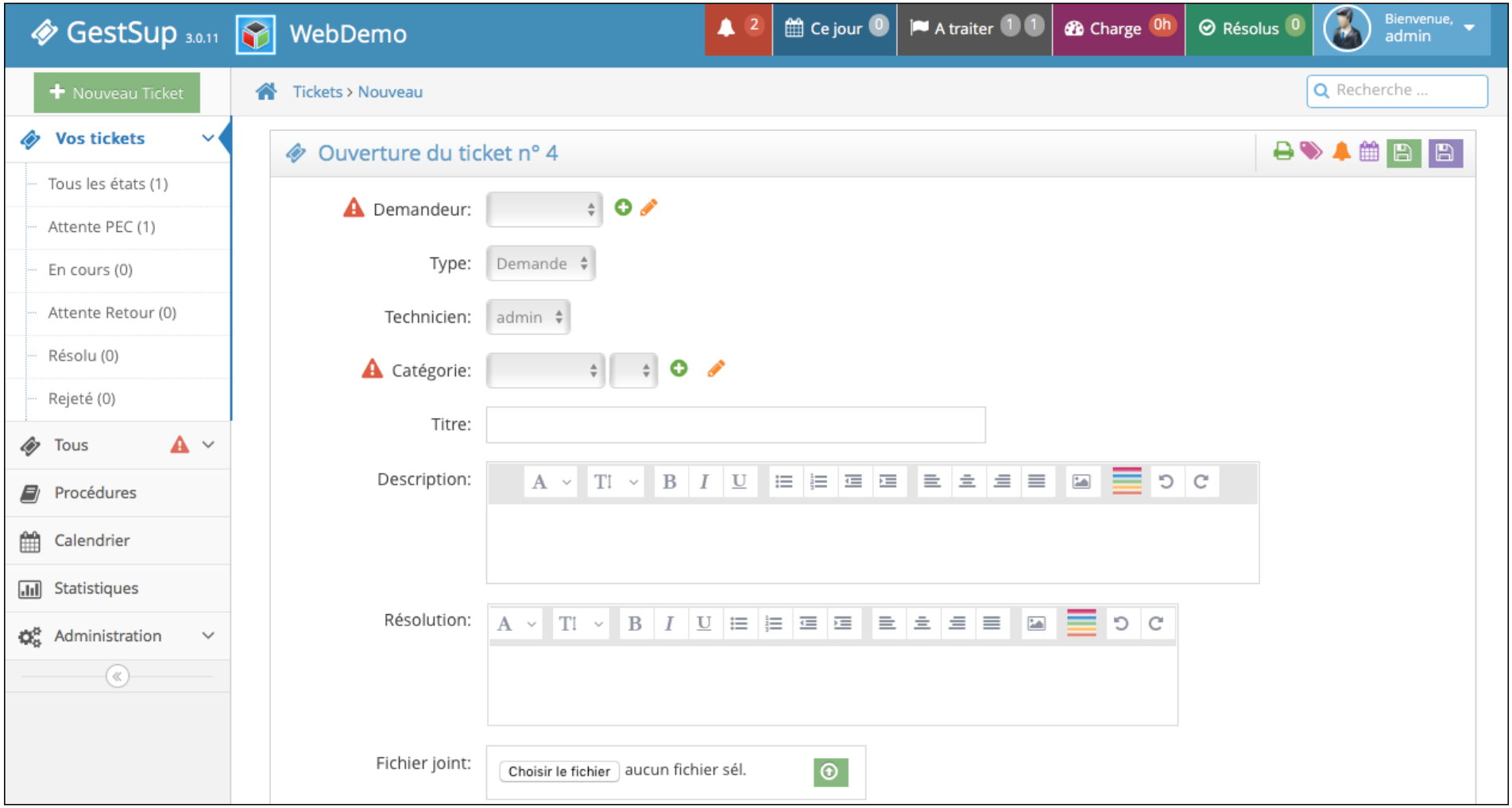
Remonté d'incidents : la solution

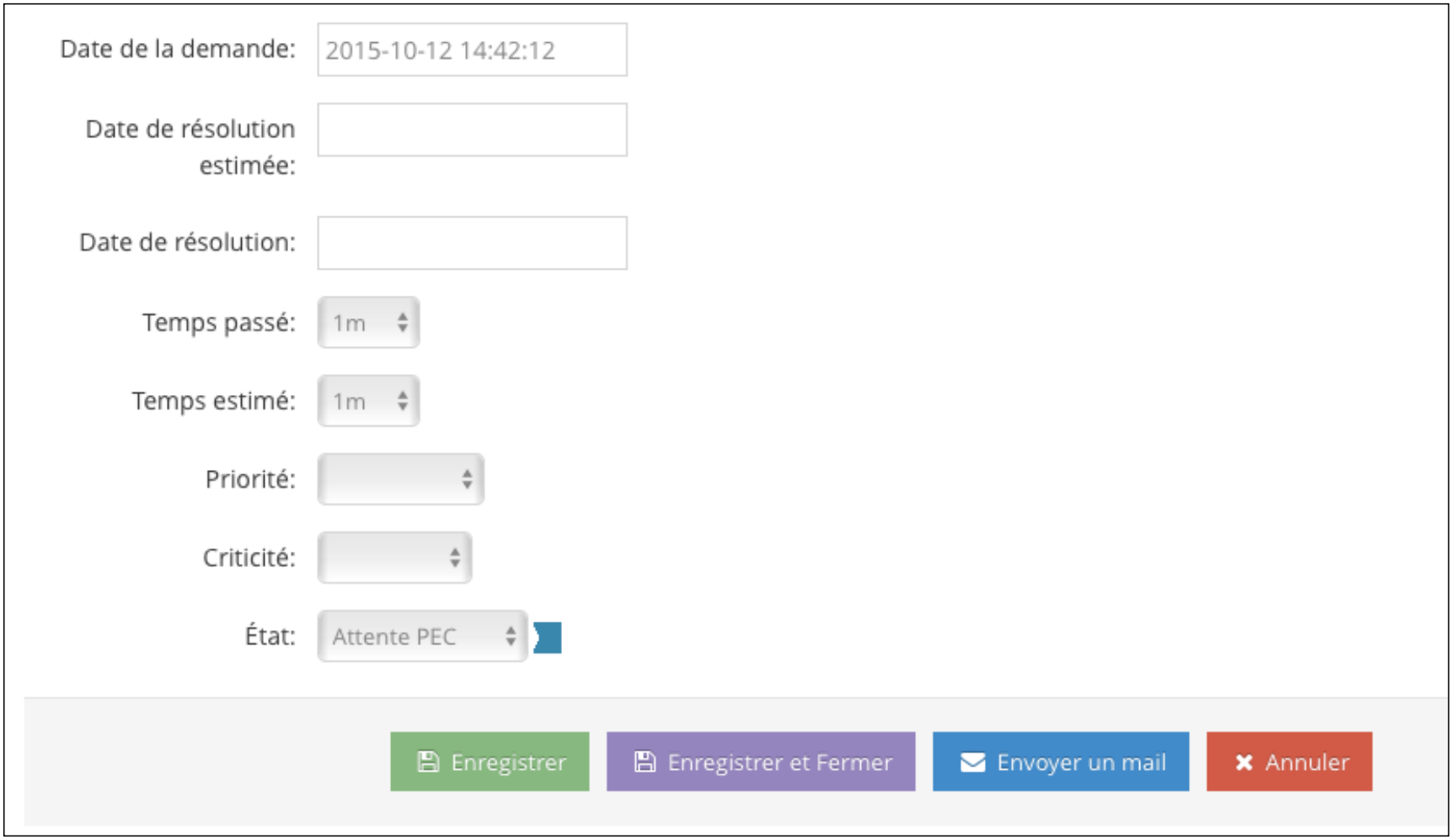
Le ticket incident

Demo

http://gestsup.fr/


GestSup 3.0.11
WebDemo
2
Ce jour 0
A traiter 1 1
Charge 0h
Résolus 0
Bienvenue, admin
Nouveau Ticket
Tickets
Recherche ...
Vos tickets
Tous les états (1)
Attente PEC (1)
En cours (0)
Attente Retour (0)
Résolu (0)
Rejeté (0)
Tous
Procédures
Calendrier
Statistiques
Administration
Tous vos tickets » Nombre: 1
Numéro
Technicien
Demandeur
Catégorie
Sous Catégorie
Titre
Date
État
Priorité
Criticité
a.
1
a.
u.
Materiel
PC
Mon poste ne démarre plus
17/03/2014
Attente PEC


GestSup 3.0.11
WebDemo
2
Ce jour 0
A traiter 1 1
Charge 0h
Résolus 0
Bienvenue, admin
Nouveau Ticket
Tickets > Nouveau
Recherche ...
Vos tickets
Tous les états (1)
Attente PEC (1)
En cours (0)
Attente Retour (0)
Résolu (0)
Rejeté (0)
Tous
Procédures
Calendrier
Statistiques
Administration
Ouverture du ticket n° 4
Demandeur:
Type:
Demande
Technicien:
admin
Catégorie:
Titre:
Description:
Résolution:
Fichier joint:
Choisir le fichier
aucun fichier sél.


Date de la demande:
2015-10-12 14:42:12
Date de résolution estimée:
Date de résolution:
Temps passé:
1m
Temps estimé:
1m
Priorité:
Criticité:
État:
Attente PEC
Enregistrer
Enregistrer et Fermer
Envoyer un mail
Annuler

Sécurité en entreprise

Quelques exemples d'attaques **en interne**

Sources : orange Business Pro, CERT

Attaques en entreprise

Etude menée par le CERT sur les menaces internes

- Secteurs les plus touchés : informatique, finance, et secteur public.
- La plupart des fraudes internes (68%) réalisées dans les trois semaines précédant le départ du fraudeur présumé
- Attaques originales

La menace vient souvent de l'intérieur

Le tour de passe-passe

- Un employé revient de nuit sur son lieu de travail
- Il échange les plaques nominatives entre son bureau et celui d'un collègue
- Il est allé demander au veilleur de nuit de lui ouvrir "son" bureau car il en avait oublié les clés.
- Il a ainsi pu copier le contenu du poste de travail du collègue.

La menace vient souvent de l'intérieur

Le contournement

- L'entreprise avait des processus de « dé-provisionnement » efficaces
- L'employé licencié le vendredi après-midi perdait immédiatement accès à tous ses comptes
- Mais accès physique n'a pas pu être révoqué avant le lundi matin
- revenu le week-end, il déclenche l'arrêt d'urgence de l'électricité dans la salle des serveurs.

La menace vient souvent de l'intérieur

Les identités multiples

- Avant d'être licencié, l'administrateur réseau a créé des comptes VPN pour le CEO et le CFO (qui n'en n'avaient aucune utilité).
- Même privé de ses accès par un processus de dé-provisionnement efficace, accès privilégié au S.I. pendant plusieurs semaines
- Sans éveil de soupçons.

La menace vient souvent de l'intérieur

Le robinet reste ouvert

- L'administrateur réseau ouvrait une connexion SSH vers une machine installée à son domicile.
- Licenciement pour faute grave avec interdiction de revenir à son poste de travail
- Tous ses accès révoqués dans la foulée
- Accès complet et privilégié au réseau chez lui
- Destruction de plusieurs systèmes d'informations

La menace vient souvent de l'intérieur

Le commentaire de trop

- Le développeur travaillant pour une société de loterie américaine avait accès aux codes sources.
- Une interface spécifique, rarement utilisée, permettait de vérifier manuellement la validité d'un billet gagnant en entrant son num. de série
- Il a pu commenter la ligne permettant d'alerter l'équipe sécurité lorsque interface était appelée.

La menace vient souvent de l'intérieur

Le verrouillage du WAN de San Francisco

- Crise entre l'administrateur et la direction (DSI), frictions entre le responsable info et l'admin
- Changement de tous les mots de passe Cisco
- Prise en otage de tous les routeurs / switchs
- http://www.journaldunet.com/solutions/securite/actualites/un-administrateur-verrouille-l-acces-au-reseau-de-san-francisco.shtml
- a fini par donner les mdp.

http://royal.pingdom.com/2009/02/20/the-inner-threat-6-cases-of-sysadmins-gone-wild/

La menace vient souvent de l'intérieur

La bombe logique

- Un employé pensant qu'il allait être viré a mis en place une bombe logique
- Script censé s'exécuter le jour de son anniversaire après son éviction
- Pas viré, mais script pas désactivé, juste repoussé
- Bombe découverte par un autre administrateur

La menace vient souvent de l'intérieur

Attaque chez UBS en 202

- Attaque d'un sysadmin sur 2000 serveurs UBS
- Suppression de milliers de fichiers
- Cause : bonus annuel plus petit qu'espéré
- Coût estimé de reprise : 3.1 millions

Want more?

http://www.cracked.com/article_19528_5-true-stories-that-prove-you-shouldnt-piss-off-it-guy.html

Minimiser les risques

- Guide bonnes pratiques.
- Ne surtout pas sous estimer ce problème
- Avoir des procédures d'ouverture et surtout de fermeture des droits efficaces
- Sensibilisation accrue à la sécurité des employés
- Bien qualifier les risques induits par certaines catégories de personnel (développeur, administrateurs réseaux systèmes)
- Renforcer le monitoring des employés.

Jamais un seul administrateur sans solution de secours en cas d'absence