Le module SISR1

Description de la ressource

Propriétés	Description
Intitulé long	Le module SISR1
Formation concernée	BTS SIO
Matière	SISR1
Présentation	Ce document présente une approche du module SISR1 du BTS SIO en proposant un bornage des savoirs ainsi que des exemples. Ces propositions, cohérentes avec le référentiel du diplôme, sont fournies uniquement à titre indicatif, elles n'ont aucun caractère contraignant pour les enseignants qui peuvent choisir de s'en inspirer ou pas.
Notions	Les notions abordées sont présentées en entête de chaque séquence proposée.
Outils	Les outils sont laissés au libre choix des professeurs.
Mots-clés	SISR1 BTS SIO Maintenance ITIL Incidents
Auteur(es)	Roger Sanchez (Relecture précieuse de Denis Gallot, Apollonie Raffalli et l'équipe SIO du CERTA)
Version	v 1.0
Date de publication	Janvier 2012

SISR1 – Maintenance des accès utilisateurs

Ce module permet de construire les savoirs et savoir-faire liés à la résolution d'incidents associés aux composants réseaux et système des solutions techniques d'accès utilisateurs.

Un incident est un événement imprévu interrompant l'accès d'un utilisateur à un service et pouvant entraîner la perte de données et/ou de communication. On s'intéresse ici aux incidents trouvant leur origine dans la partie système ou dans la partie réseau des solutions techniques d'accès utilisateurs.

Remarques :

- Ce module s'inscrit plus particulièrement dans le processus « fourniture de services » (P2) en prenant appui sur le processus « Conception et maintenance des solutions d'infrastructures » (P3) mais la répétition cyclique d'un même incident peut conduire à une nouvelle « Production de services » (P1) via la gestion des problèmes et des changements.
- Ce module s'appuie sur les savoirs et savoir-faire vus dans les modules SI1 et SI2
- La maintenance des accès utilisateurs doit s'entendre dans une dimension préventive et corrective.
- Les incidents à prendre en compte peuvent avoir été provoqués par des dysfonctionnements matériels ou logiciels, des erreurs d'utilisation ou des outils malveillants.
- Les incidents sont associés, soit à la dimension système et matériel des solutions techniques d'accès (SI1), soit à l'infrastructure réseau d'accès (SI2).
- Un incident ne se réduit pas à la seule interruption de service mais comprend aussi la dégradation de la qualité d'un service.
- La prise en compte des incidents doit respecter autant que faire se peut une procédure professionnelle permettant notamment de garder une trace de l'incident et de sa résolution et donc prendre appui sur un logiciel de gestion d'incidents incluant une base de connaissances et sur un logiciel de gestion de parc.
- Les normes et standard associés à la gestion des incidents doivent être étudiés.
- On doit veiller avant tout à restaurer l'environnement de travail de l'utilisateur sans perte de données en minimisant le temps d'interruption de service. On peut donc être amené à dissocier parfois le retour à la fourniture d'un service opérationnel et le diagnostic de l'incident.

La construction proposée ici st la suivante :

- **Prévenir** (configurer, sauvegarder, surveiller, intervenir)
- **Corriger** (détecter, diagnostiquer, réparer, valider et documenter)
- **Gérer** (outils gestion de parc, gestion d'incidents, politique de maintenance, périmètre d'intervention, normes)

Prévenir est un approfondissement avec un déplacement du « focus » de notions vues en SI1 et SI2 mais avec introduction de notions nouvelles.
Corriger (ou réparer) s'intéresse plus particulièrement au diagnostic et doit permettre de poser une méthodologie de résolution des problèmes.
Gérer prend du recul et introduit les normes et standards associés à la gestion des incidents.

En fonction des objectifs qu'on se fixe, les séquences peuvent être plus ou moins approfondies, on peut par exemple vouloir passer plus de temps sur la partie **Corriger** ou **Gérer** que sur la partie **Prévenir.**

Renvoyer l'étude des outils et des normes en fin de progression peut permettre de privilégier la mise en place de séquences éducatives intéressantes assez rapidement.
Mais on peut cependant estimer à juste titre qu'il faut présenter les normes et standards associés à la gestion des incidents au plus tôt et faire utiliser rapidement des outils de gestion de parc et d'incidents.

On pourra s appuyer avec intérêt sur les éléments suivants :

Certifications Windows Seven

- http://www.microsoft.com/learning/fr/fr/Exam.aspx?ID=70-685&locale=en-us#tab2
- http://www.microsoft.com/learning/fr/fr/certification/certification-windows-7-client.aspx#tab4

Documents Ubuntu

- http://doc.ubuntu-fr.org/reparer_ubuntu

Cisco

- http://cisco.netacad.net/cnams/content/templates/LibraryHome.jsp?#/resource/lcms/cnams_site/english/generic_site_areas/library/Course_Resources/ccna-exp-wan/Chp8.html

Quelques labs CISCO intéressants ;

- Che1_IG_Lab_9.2.7.3-Trblsh-Using-Net-Utils
- Che1_IG_Lab_9.3.3.2-Trblsh-Phys-Conn

ITIL

- http://itil-france.com/pages/docs/hgelun/itilv2_incidents.pdf
- http://www.itilfrance.com/index.php?pc=pages/docs/glossaire/index.inc&pg=menu_accueil.inc&pt=Glossaire&pb=haut_accueil_glossaire.inc
- http://www.itilfrance.com/index.php?pc=pages/docs/itilv2/10-1-index_cds.inc&pg=menu_itilv2.inc&pt=Le%20centre%20de%20services

Rapports du CLUSIF (orienté sécurité)

- http://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF-2011-Gestion-des-Incidents.pdf

Une réflexion intéressante sur la méthodologie de diagnostic

- http://www.ista.ma/remos_downloads/TSSRI_Systeme_et_Reseaux_Informatiques/M09_Depannage_de_premier_niveau_d-un_reseau_local/Methode_de_depannage_en_informatique.1149.pdf

Reseau Certa

- http://www.reseaucerta.org/cotelabo/cotelabo.php?num=523 (Automatisation de l'inventaire d'un parc informatique avec télé-déploiement d'application ; gestion des demandes d'assistance ; gestion comptable et financière des équipements)

- http://www.reseaucerta.org/cotelabo/cotelabo.php?num=553 (PowerShell : procédure rapide de réinstallation de postes de travail Windows 7)

Revue

- Linux Pratique N°69 de Janvier/février 2012 « Comment survivre à un crash système sans paniquer - Redo Backup and recovery : solution simple et rapide pour sauver et restaurer vos données pour Linux ou Windows »

Document

Un document intéressant (déniché par Serger Guérinet) qui nous montre que la gestion des incidents ne date pas d'hier

- http://www.c-log.com/product/opd/more/Incident.pdf

Prévenir

Savoirs et savoir-faire	Notions	Travaux dirigés	Activités en laboratoire
- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents - Technique d'assistance aux utilisateurs	**Objectif :** Anticiper la résolution des incidents par une politique de configuration des solutions techniques d'accès - Protection du système dans l'utilisation courante (habilitations) : Qui a droit à quoi ? Vérifier et documenter les habilitations des utilisateurs en fonction des choix organisationnels. Quelle politique de droits et de privilèges ? - Protection du système contre les malveillances : (antivirus, antispyware…) => identifier les risques, définir les outils - Mise à jour du système (Pourquoi mettre à jour son système ? Mise à jour automatique ? Versions ? Précautions) - Nettoyage du système (Nettoyage ? Supprimer des fichiers ? Supprimer des applications ? Supprimer un utilisateur ? etc.) - Industrialisation d'une politique de configuration. - Veille technologique et informations sur les risques (quelle veille ? Quels sites ? .etc.)	- Établir une typologie des logiciels malveillants (adware, drive by download, redirecteur de page, spam, spyware, dialer, trojan, virus, keylogger…). Tester un antivirus avec le vrai-faux virus EICAR. - À partir des documents du CERT définir ce qu'est l'obsolescence d'un système ou d'un logiciel et le risque pris en continuant à l'utiliser, déterminer les termes d'alerte et de vulnérabilité	**Mise en œuvre d'une politique de configuration** : Exécuter un script au démarrage de session. Interdire ou autoriser l'utilisation d'une application. Restreindre l'accès au panneau de configuration. Configurer un firewall personnel. Configurer les mises à jour. Configurer une tâche planifiée pour nettoyer le système à l'ouverture de session. Ouvrir Comptes utilisateurs avec une ligne de commandes. Récupérer l'accès perdu aux comptes utilisateurs…
- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents - Technique d'assistance aux	**Objectif :** Anticiper la résolution des incidents par la mise en place de solutions de récupération - Utilisateurs :	- Environnement utilisateur (stockage des paramètres utilisateurs, stockage local ou centralisé.	**Récupération de données**. De la sauvegarde/restauration, aux clichés de volume avec point de restauration et autres utilitaires pour récupérer des données, etc. (Windows et/ou Linux, outils de fileRecovery).

utilisateurs - Technique de sauvegarde et de restauration d'un environnement - Installer une solution de sauvegarde et de restauration de l'environnement - Restaurer un environnement	○ Paramètres de configuration (profils, environnement, paramétrage des applications) ○ Données utilisateurs (documents bureautiques, fichiers de travails, dossiers personnels, etc.) ○ Suppression de données (logique, physique, trace) ○ Corruption de données (audit) ○ Sauvegarde et restauration de données utilisateurs, anticipation des pertes données par des systèmes permettant le retour arrière après effacement de documents : « clichés instantanés », gestion de différentes versions d'un même document - Système ○ Applications ○ Services ○ OS - Sauvegarde et restauration du système	- Environnement système (stockage de paramètres applicatifs et système)	Suppression physique et logique. Audit de données. Trace sur un système
- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents - Technique d'assistance aux utilisateurs - Technique de sauvegarde et de restauration d'un environnement - Installer une solution de sauvegarde et de restauration de l'environnement - Restaurer un environnement	**Objectif :** Anticiper la résolution des incidents par la mise en place d'une politique de surveillance - Journaux systèmes et applicatifs (quelles informations ? Comment lire un journal d'activité) - Services réseaux ouverts (rappels sur la notion de port et d'écoute ? Pourquoi est-il important de vérifier les ports ouverts). - Audits d'activité (pourquoi auditer ? Quels objets audités ? Quels événements audités ?)	- Déclencher une action (par exemple : envoi de mail) en fonction d'un événement (ex : disque dur saturé). Collecter les événements sur un serveur d'événement. (avec Linux voir Syslog et syslogd). Activer l'audit d'un objet. Écrire un script de démarrage qui audite les ouvertures	**Restauration de système**. Créer un disque Winre sous Windows Seven. Casser un système et le restaurer (http://www.webastuces.net/astuces/cd-de-recuperation-windows-7-winre/). Utiliser une distribution spécialisée sous Linux (System rescue CD, Recovery is possible, Redo Backup et discovery, etc.)

	- Indicateurs d'activité (quels indicateurs retenir ? Quelles valeurs « cibles » pour ces indicateurs ? Quel seuil d'alerte ?)	de sessions (auditpol.exe sur W7). - Découvrir les services réseaux à l'écoute (utilitaires et commandes)	
- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents - Technique d'assistance aux utilisateurs - Installer, configurer et utiliser un logiciel de prise de contrôle à distance	**Objectif :** Anticiper la résolution des incidents par la mise en place de solutions d'intervention sur site ou à distance - Comptes administrateurs locaux, accès au BIOS - Prise de contrôle à distance o Principe o outils o protocoles - Utilisation d'un langage de commandes à distance o SSH o Powershell - Sécurité de la prise de commande à distance - Authentification - Autorisation - Confidentialité	- Recherche d'outils de contrôle à distance (caractéristiques, avantages et inconvénients) - Principe d'une « tunnelisation» SSH.	- **Prise de contrôle à distance** sécurisée en mode commande et graphique. Installation, configuration, utilisation. Mise à jour du firewall personnel pour autorisation de la prise de contrôle à distance. - **Assistance à distance** à un utilisateur

Réparer

Savoirs et savoir-faire	Notions	Travaux dirigés	Activités en laboratoire

- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents
- Technique d'assistance aux utilisateurs
- Gestion des priorités et d'organisation du temps de travail
- Établir un diagnostic et appliquer une méthode de résolution
- Prendre en charge la déclaration d'un incident ou d'une demande d'assistance à l'aide d'un logiciel ad hoc
- Valider et documenter la résolution d'un incident
	Objectif Traiter l'incident
	- Détecter l'incident (repérer la conséquence -symptôme - de l'incident)
	  ○ Dégradation de services
	  ▪ Qu'est ce qu'une dégradation de service ? Exemples : symptômes et origines possibles
	  ○ Interruption de services
	  ▪ Qu'est ce qu'une interruption de services ? (au sens large, la perte de données, la malveillance sont incluses ici) Exemples : symptômes et origines possibles
	  ○ Dialogue avec utilisateur
	  ▪ Règles à respecter (courtoisie, rassurer, empathie .etc.)
	  ▪ Stratégie de questionnement
	  ○ Enregistrement de l'incident dans un logiciel de gestion d'incidents
	  ▪ Rôle d'un logiciel de gestion d'incidents (assez rapide car revu plus loin)
	  ▪ Différents outils
	- Diagnostiquer (repérer la cause de l'incident)
	  ○ Rechercher des informations sur des sites spécialisés
	  ○ Localisation
	  ▪ Matériel
	  ▪ Application
	  ▪ Système
	  ▪ réseau
	  ○ Repérer l'élément défaillant (check-list)
	  ○ Classer l'incident en fonction du niveau d'information
		- Établir un questionnement utilisateur à partir de différents exemples de déclaration d'incidents (le TD peut se faire à 2)
		- Scénarisation : à partir de listes de symptômes ; établir une liste hiérarchisée d'hypothèses correspondantes
		- Jeu de rôle : simuler par exemple la remontée d'un incident au téléphone
			Gérer un problème au démarrage du système. Incidents sur le POST. Gestion BIOS. Étude du système de BOOT de 2 OS différents (Gestionnaire de BOOT Windows BCD et GRUB sous Linux. Récupération des informations de démarrage avec msconfig.exe sous Windows. BootChart ou Dmesg sous Linux. Démarrer en mode commande dans les 2 systèmes. Modifier la séquence de démarrage (bcdedit.exe, Bootrec.exe .etc.) …

	○ Choisir une procédure de résolution d'incident - Résoudre et clôturer l'incident (réparer) ○ Mettre en œuvre une procédure de résolution ○ Valider le retour à une situation conforme au contrat de service (tests, contrôle de qualité, etc.) ○ Documenter et enregistrer le traitement de l'incident		
- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents - Technique d'assistance aux utilisateurs - Gestion des priorités et d'organisation du temps de travail - Établir un diagnostic et appliquer une méthode de résolution - Remplacer les éléments matériels ou logiciels défectueux ou obsolètes - Restaurer un environnement - Prendre en charge la déclaration d'un incident ou d'une demande d'assistance à l'aide d'un logiciel ad hoc - Valider et documenter la résolution d'un incident	**Objectif :** Diagnostiquer un incident réseau - Utilitaires réseau (ping, tracert, netstat, nbtstat, netsh, etc.) (Windows et/ou Linux) - Incidents de connectivité ○ Connexion physique (filaire et non filaire) ○ Adressage (fixe, dynamique) ○ Résolution de noms (DNS, Netbios) ○ Routage ○ Accès internet (proxy, NAT .etc.) - Incidents d'accès aux ressources ○ Groupe de travail et/ou domaine (intégration à un groupe, authentification, etc.) ○ Accès aux ressources partagées	- Commandes réseaux (explorer ici les options intéressantes de chaque commande) - Création d'un partage (rappels sur ACL et authentification)	**Créer une ou plusieurs pannes réseau**. Détection de la panne, diagnostic, résolution, documentation. On peut imaginer des scénarii à 2 étudiants. Chaque étudiant mettant en place un environnement ne fonctionnant pas qu'un autre étudiant doit dépanner..Quelques exemples : désactiver un port de commutateur et connecter un poste sur le port désactivé, Dégrader le vitesse du port. Générer des conflits d'adresses IP...)
- Technologies, techniques et méthodes associées au diagnostic	**Objectif :** Diagnostiquer un incident	- Commandes système (explorer ici	**Créer une ou plusieurs pannes système**. Détection de la panne,

et à la résolution d'incidents - Technique d'assistance aux utilisateurs - Gestion des priorités et d'organisation du temps de travail - Établir un diagnostic et appliquer une méthode de résolution - Remplacer les éléments matériels ou logiciels défectueux ou obsolètes - Restaurer un environnement - Prendre en charge la déclaration d'un incident ou d'une demande d'assistance à l'aide d'un logiciel ad hoc - Valider et documenter la résolution d'un incident -	système - Utilitaires système o Invite de commande et langage de commandes o Utilisation distante du langage de commandes o Commandes d'informations sur matériels, utilisateurs, ressources o Journaux d'activité o Moniteurs de ressources / analyseur de performance - Incidents matériel o Carte mère (codes POST, alimentation, processeur, mémoire .etc.) o Périphériques d'E/S o Périphériques de stockage - Incidents système o Démarrage (retour sur TP précédent) o Variables d'environnement o Principaux fichiers système o Processus o Services système o Restauration (retour sur TP précédent)	quelques commandes intéressantes, ex windows secedit .etc.) - Utilisation du moniteur système (windows et/ou Linux	diagnostic, résolution, documentation. Le réseau fonctionnant, on diagnostiquera et réparera en prenant la main à distance de façon sécurisée en mode commande
- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents - Technique d'assistance aux utilisateurs - Gestion des priorités et d'organisation du temps de travail - Établir un diagnostic et appliquer une méthode de résolution - Remplacer les éléments matériels	**Objectif :** Diagnostiquer un incident applicatif - Application o Rappels sur la notion d'application o Fichiers associés à une application (exécutables, paramètres systèmes, paramètres utilisateurs, journaux d'activités, répertoires d'installation, d'exécution .etc.) o Étude d'applicatifs standards o Bureautique o Navigateur o Client messagerie - Incidents d'utilisation	- Étude et paramétrage des applications bureautiques standard - Paramétrage de la sécurité d'un navigateur	**Créer une ou plusieurs pannes applicatives** ou défaut d'utilisation. Détection de la panne, diagnostic, résolution, documentation. Le réseau fonctionnant, on diagnostiquera et réparera en prenant la main à distance de façon sécurisée en mode graphique. On peut imaginer aussi ici des scénarii d'assistance utilisateur

ou logiciels défectueux ou obsolètes - Restaurer un environnement - Prendre en charge la déclaration d'un incident ou d'une demande d'assistance à l'aide d'un logiciel ad hoc - Valider et documenter la résolution	○ Mauvais paramétrage, droits inappropriés, etc. ○ Ajouts de fonctionnalités bloquantes (codecs, flash .etc.) ○ Mauvaise utilisation (assistance utilisateur) - Incidents associés aux malveillances ○ Risques associés aux logiciels standards ○ Détection de comportement malicieux ○ Veille technologique, informations des utilisateurs ○ Protection des logiciels standards (antivirus, antispam, antiphishing .etc)		

Gérer

Savoirs et savoir-faire	Notions	Travaux dirigés	Activités en laboratoire
- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents - Technique d'assistance aux utilisateurs - Gestion des priorités et d'organisation du temps de travail - Établir un diagnostic et appliquer une méthode de résolution - Prendre en charge la déclaration d'un incident ou d'une demande d'assistance à l'aide d'un logiciel ad hoc - Valider et documenter la résolution d'un incident	**Objectif :** Définir le périmètre d'intervention et le documenter - Situer le niveau de responsabilité du service de gestion des incidents => Quels incidents doit-on résoudre ? Qui résout les autres incidents ? (exemple : vol de données, malveillance d'un utilisateur, défaillance d'un serveur, etc.) ? Niveaux de maintenance (voir aussi doc CLUSIF) - Quels matériels ? Quels systèmes ? Quels logiciels ? Quels actifs réseaux ? => peut-on tout connaître ? Connaître l'environnement maintenu : le système et sa configuration, le réseau et sa configuration, les applicatifs utilisateurs, etc. - Documenter la configuration des solutions techniques d'accès en fonction des habilitations des utilisateurs (droits, privilèges, permissions, restrictions, etc.) - Documenter la configuration des accès réseaux et disposer d'un schéma réseau => quels éléments doit-on prendre en compte ? Que permet chaque élément ? (s'il y a un problème sur un élément donné, que se passe-t-il ?) - Inventorier les configurations matérielles et logicielles (les outils d'inventaire et de gestion de parc : rôle, fonctionnement, architecture, exemples, etc.)	- Documenter la configuration réseau des STA de la salle de formation - Documenter la configuration système et applicative des STA de la salle de formation	**Utiliser un logiciel de gestion de parc**
- Technologies, techniques et méthodes associées au diagnostic et à la résolution d'incidents - Technique d'assistance aux utilisateurs	**Objectif :** Définir une politique de maintenance - Définir les différents types de maintenance - Préventive, corrective, curative, palliative,	- Évaluer le cout d'un service de gestion des incidents - Présenter un problème récurrent (exemple installation par les utilisateurs de programmes non conformes) et proposer et évaluer	**Utiliser un logiciel de gestion d'incidents**

- Gestion des priorités et d'organisation du temps de travail - Établir un diagnostic et appliquer une méthode de résolution - Prendre en charge la déclaration d'un incident ou d'une demande d'assistance à l'aide d'un logiciel ad hoc - Valider et documenter la résolution	systématique, conditionnelle, prévisionnelle, etc. - Réfléchir à une théorie du diagnostic - Symptômes, hypothèses, etc. - Déterminer les impacts sur la sécurité de la gestion des incidents - Étudier les normes et standards associés à la gestion des incidents (ITIL, COBIT, etc.) - Passer d'une gestion des incidents à une gestion des problèmes - Étudier les outils associés à la gestion des incidents (rôle, principes, architecture, utilisation, exemples, etc.)	une solution pour résoudre le problème	