**Modèle de matrice de remontée des problèmes
pour le service informatique/ITIL - Exemple**



Échec d’installation de logiciel

En tant que premier point de contact en cas de problème informatique, le système d’assistance informatique s’occupe des questions d’ordre général et des résolutions de problèmes basiques.

Le niveau 2 gère les questions plus complexes qui nécessitent des connaissances spécialisées ou des compétences techniques supplémentaires.

Le niveau 3 gère les défis techniques de haut niveau impliquant l’infrastructure système ou des problèmes logiciels complexes.

**Service d’assistance informatique (niveau 1)**

Le niveau X correspond à une assistance externe spécialisée ou à une assistance spécifique au fournisseur concernant des questions très spécifiques.

**Assistance de niveau 2**

**Assistance de niveau 3**

**Assistance de niveau X**

Temps d’arrêt du réseau

Atteinte à la sécurité des données

Interruptions du service cloud

Confirmer la configuration système et tenter des procédures de réinstallation de base.

Effectuer des diagnostics détaillés pour identifier les conflits ou les fichiers corrompus. Effectuer des tests sur d’autres systèmes, le cas échéant.

Vérifier et corriger les paramètres profonds du système ou les conflits de registre qui pourraient empêcher le système de sécurité de fonctionner.

Contacter le fournisseur du logiciel en cas de problèmes d’installation de logiciels propriétaires ou pour recevoir des correctifs.

Vérifier les rapports initiaux et confirmer si le problème est général ou localisé. Réinitialiser les routeurs ou les commutateurs, le cas échéant.

Analyser les journaux réseau et collaborer avec les fournisseurs d’accès à Internet ou les équipes en charge du réseau interne pour localiser les perturbations.

Mettre en œuvre des procédures avancées de récupération du réseau et reconfigurer les principaux protocoles de routage.

Faire appel aux fournisseurs d’équipements réseau à des fins de mise à jour critique des micrologiciels ou de diagnostics spécialisés.

Consigner l’incident, alerter les équipes de sécurité et lancer une procédure préliminaire de verrouillage des données.

Effectuer une première analyse pour évaluer l’ampleur de la violation et identifier les systèmes compromis.

Mener des audits de sécurité complets et mettre en œuvre des stratégies de remédiation afin de sécuriser tous les points de données.

Travailler avec des entreprises de cybersécurité pour mettre au point des solutions de détection des menaces et des techniques d’atténuation.

Vérifier le statut des services auprès des fournisseurs de services cloud et communiquer les détails des pannes aux utilisateurs.

Évaluer les intégrations API et vérifier les services connexes pour assurer la connectivité.

Coordonner avec les ingénieurs cloud la restauration des services et gérer les contrôles d’intégrité des données.

Communiquer avec les fournisseurs de services informatiques cloud afin de procéder à une analyse détaillée des causes profondes et d’éviter toute interruption future.

|  |
| --- |
| **EXCLUSION DE RESPONSABILITÉ**Tous les articles, modèles ou informations proposés par Smartsheet sur le site Web sont fournis à titre de référence uniquement. Bien que nous nous efforcions de maintenir l’information à jour et exacte, nous ne faisons aucune déclaration, ni n’offrons aucune garantie, de quelque nature que ce soit, expresse ou implicite, quant à l’exhaustivité, l’exactitude, la fiabilité, la pertinence ou la disponibilité du site Web, ou des informations, articles, modèles ou graphiques liés, contenus sur le site. Toute la confiance que vous accordez à ces informations relève de votre propre responsabilité, à vos propres risques. |