Opsgenie

Le jargon de la gestion des incidents

Introduction

Le jargon utilisé dans l'écosystème de la haute technologie est pour le moins dynamique. Aucun autre secteur n'utilise un tel brassage de jargon technique, parfaitement imbriqué avec des références issues de la science-fiction, de la mythologie, de la culture pop, de la littérature, et bien plus encore.

Si les conversations dans les environnements techniques n'en deviennent que plus colorées et intéressantes, les communications sont, elles aussi, allégoriques et métaphoriques, les ouvrant à une interprétation variable.

Lorsque la communication est plus détendue, ce style de conversation peut être considéré comme stimulant et ludique. Cependant, en cas d'incident, le niveau de gravité change, et un tout autre jargon fait son apparition. Compte tenu de l'impact potentiellement énorme des incidents informatiques sur les opérations business, le jargon de la gestion des incidents doit être techniquement précis, exploitable et ne laisser aucune place à une interprétation erronée.

Pourquoi ce virage dans la communication est-il nécessaire ? Parce que les opérations informatiques modernes sont au cœur des opérations business. Si un système tombe en panne, l'impact est immédiat et considérable, chaque minute d'arrêt coûtant des dizaines voire des centaines de milliers de dollars.

Avec un tel niveau de gravité, il est logique que bon nombre des termes utilisés de nos jours dans la gestion des incidents informatiques soient directement repris du vocabulaire largement adopté par les équipes de réponse aux catastrophes. Un vocabulaire clair et compréhensible dans des environnements chaotiques, qui aide les équipes à travailler ensemble pour remédier à un incident le plus rapidement possible.

Ce livre blanc a été créé pour servir de base aux équipes afin d'améliorer la communication pendant toute la durée d'un incident. Il met en évidence et définit les termes essentiels, qui aident à favoriser une communication claire et précise lors d'un incident.

Pour plus de précisions, ces termes ont été classés en fonction des cinq phases du cycle de vie des incidents où ils sont le plus susceptibles d'être utilisés. Ces phases sont les suivantes : **planification, détection et alerte, maîtrise, résolution/remédiation** et **analyse**, et sont indiquées par une icône correspondante, décrite dans la clé ci-dessous.

* Pour plus d'informations sur les différentes phases d'un incident, téléchargez le livre blanc « Les cinq phases de la gestion des incidents et comment les améliorer ».

Index

Planification

Phase de la gestion des incidents durant laquelle les incidents sont anticipés et les processus de résolution/remédiation sont pensés à l'avance.

Détection et alerte

Phase de la gestion des incidents au cours de laquelle les incidents sont portés à la connaissance de tous les services concernés.

Maîtrise

Phase de la gestion des incidents au cours de laquelle un incident a été détecté, et où les efforts visent à s'assurer qu'il n'affecte aucun autre service ou fonction.

Résolution/Remédiation

Connue également sous le nom de « remédiation » ou de « rattrapage » (ITIL). Phase de la gestion des incidents au cours de laquelle des mesures correctives sont prises pour résoudre un incident.

Analyse

Phase de la gestion des incidents au cours de laquelle un incident a été résolu et doit maintenant être inspecté pour améliorer encore la résilience, le processus de résolution/remédiation, et bien plus encore.

A

Accès concurrents	Mesure des événements identiques qui se produisent simultanément dans un système, par exemple le nombre d'utilisateurs qui accèdent à la même opération ou effectuent la même transaction.	
Accord sur les niveaux de service (SLA)	Engagement pris entre un fournisseur de services et un consommateur ou un client. Cet accord définit les attentes en matière de qualité ou de fonctionnalité ciblée.	
Actif immobilisé	Actif corporel du business ayant un long terme de service. Un bureau, un ordinateur ou une licence peuvent être considérés comme des actifs immobilisés.	
Actif/Gestion des actifs	Composants de tout système ou réseau ayant une valeur business. Ces composants sont gérés de manière à comprendre l'impact de l'actif lorsque l'on décide de le supprimer ou de le mettre à jour, par exemple.	

A

Alerte **· Alerte de l'intervenant** **· Alerte du propriétaire** **· Alerte associée**	Alarme ou avertissement déclenché(e) pour un événement susceptible d'affecter des opérations ou un service. · Alerte envoyée aux parties/à l'équipe directement responsables de prendre des mesures. · Alerte qui indique à quelle équipe appartient le service concerné. · Alerte qui représente une partie, ou un symptôme, d'un événement ou d'un incident plus vaste.	
Alerte exploitable	Alerte qui décrit clairement un problème, est acheminée aux bonnes personnes au moment opportun et communique non seulement l'urgence, mais aussi l'ampleur de l'impact.	
Alerte non exploitable	Alerte qui ne permet pas à un intervenant de prendre des mesures. Elle manque souvent d'informations contextuelles, est acheminée aux mauvaises personnes, et son périmètre est imprécis.	
Analyse de Kepner & Tregoe	Méthode de résolution des problèmes qui évalue tous les aspects d'un problème, indépendamment d'une décision finale concernant la cause. L'objectif de cette analyse est de déterminer la cause après avoir parfaitement cerné le problème.	

A

Analyse de la valeur de dérangement	Processus permettant d'identifier l'impact des incidents. Cette formule est généralement basée sur plusieurs facteurs : durée de l'incident ou de l'interruption/la panne, utilisateurs affectés, coût, etc.	
Analyse de tendance	Investigation sur les schémas relatifs au temps.	
Analyse des défaillances de service (SFA)	Processus qui consiste à inspecter une interruption de service pour en déterminer la cause. Cela permet d'étudier les possibilités d'améliorer la résilience d'un service informatique.	
Analyse d'impact de la défaillance de composants (CFIA)	Processus consistant à déterminer l'impact sur un service lorsqu'un composant ou un élément de configuration cesse de fonctionner comme prévu.	
Analyse d'impact sur le business	Évaluation systématique de l'effet potentiel d'une indisponibilité ou interruption d'un service sur le business, et besoins de reprise en cas d'incident de ce type.	
Analyse par arbre de pannes (FTA)	Technique utilisée pour déterminer les différents événements qui ont conduit à un incident. Cette analyse est utilisée pour prévoir ce qui pourrait causer des incidents à l'avenir et est souvent appliquée pour essayer de déterminer la cause première.	

A

Analyse post-mortem/ post-incident	Processus visant à comprendre un incident après sa résolution dans le but d'améliorer les processus de réponse ou de comprendre la causalité.	
Assurance qualité (QA)	Processus de test permettant de s'assurer que les normes sont respectées pour tout ce qui a trait à l'informatique, des instructions de documentation à une nouvelle fonctionnalité.	
Audit	Examen formel d'un système ou d'un processus qui vérifie la disponibilité et l'utilisation du système, et/ou si les directives et les politiques sont suivies.	

B

Base de référence	Point de référence pour le comportement attendu afin de mesurer les changements, les améliorations, ou à utiliser comme point de restauration si le changement ou l'amélioration provoque une défaillance.	
Benchmark/ Benchmarking	Point de référence qui fonctionne comme une base de référence pour mesurer les progrès réalisés par rapport aux benchmarks passés et à d'autres données comparatives.	

B

Bruit d'alerte	Résultat d'une quantité écrasante d'alertes créées en peu de temps, ce qui complique la capacité des intervenants à identifier avec précision les services concernés.	
Bug	Problème involontaire dans un logiciel, un code, des programmes, etc. susceptible d'entraîner une défaillance ou un comportement anormal.	

C

Capacité	Mesure du débit maximal pouvant être transféré entre les réseaux ou fourni par un service.	
Cause première	Généralement considérée comme la véritable raison unique de la défaillance d'un service ou d'une application. Toutefois, de nombreux facteurs contribuent aux défaillances et aux interruptions/pannes, de sorte que l'utilisation de ce terme est discutable, car il peut être potentiellement trompeur lorsque plusieurs facteurs sont interconnectés dans la cause d'un incident.	
Centre de services	Service ou équipe de personnes qui reçoit les demandes d'assistance des clients, et sert de point de contact entre les clients et le personnel informatique interne.	

C

Changement **· Historique des changements** **· Gestion des changements**	Tout changement apporté à un service, une configuration, un réseau ou un processus informatique, dont le périmètre inclut la documentation. Inventaire complet des altérations apportées à l'un des éléments ci-dessus depuis le début de son cycle de vie jusqu'à son état actuel. Méthode permettant de contrôler l'ensemble de l'historique et du cycle de vie des changements pour comprendre quels changements ont entraîné des améliorations globales, et pour minimiser la possibilité et l'impact de tout incident lié au changement.	
Changement normal	Mise à jour/correction attendue qui suit le processus de gestion des changements, et qui n'est pas effectuée en cas d'urgence ou comme solution de contournement.	
Changement urgent	Mise à jour ou correctif à déployer rapidement, généralement dans le cadre des efforts de résolution des incidents.	
Charge de travail	Ressources (temps, et travail humain et mécanique) nécessaires pour fournir un service informatique.	

C

ChatOps	Exploitation des outils de chat et de collaboration dans le cadre de la gestion des incidents, en particulier pour automatiser les mesures et la recherche d'informations complémentaires.	
Chronologie	Liste complète des événements qui se produisent, des changements/corrections appliqués, des résultats, etc., et moment où ils se sont produits au cours d'un incident.	
Code de bonne pratique	Guide de bonnes pratiques qui exprime les normes de conduite des affaires et reflète les objectifs d'une entreprise.	
« Cold standby » (Reprise graduelle)	Option de reprise dans laquelle la récupération attendue devrait prendre plusieurs jours voire semaines. Les infrastructures sont provisionnées, mais le matériel et les logiciels ne sont pas inclus dans cette option de reprise.	
Configuration	Agencement d'éléments ou de services qui contribuent à fournir un résultat déterminé.	
Conformité	Fait de suivre les règlements en vigueur. Peut déclencher une alerte si un système ou un élément de configuration n'est pas conforme.	

C

Contexte	Événements ou environnement périphériques, qui fournissent des informations pertinentes sur un incident ou une alerte.	
Contre-mesure	Mesure réactive spécifique, prise dans le but de protéger un système ou de rétablir les opérations.	
Contrôle, contrôler	Procédures et politiques qui gèrent les risques, et garantissent que le produit ou le service fonctionne comme prévu et que la conformité est respectée.	
Copie de sauvegarde	Copie stockée des données, ou système redondant disponible pour être utilisé au cas où le système d'origine serait compromis ou perdu.	
Correction	Mesure ou méthode de réparation.	
« Cycle de vie » d'un incident	Série de changements que subit une alerte/un incident, de sa création à sa résolution.	

D

De secours	Ressources non utilisées de façon active, mais toujours disponibles pour soutenir les plans de continuité des services informatiques.	

Planification · Détection et alerte · Maîtrise · Résolution/Remédiation · Analyse

D

Défaillance	État de fait dans lequel un élément ayant un résultat attendu cesse de fonctionner et de fournir ce résultat.	
Dégradation des performances	Mesure de la diminution des performances d'un élément lié à l'informatique en raison d'un événement.	
Délai moyen de réparation (MTTR)	Mesure du temps moyen entre la notification initiale et la résolution/remédiation finale d'un problème.	
Délai moyen de restauration du service (MTRS)	Mesure du temps moyen nécessaire pour rétablir la fonctionnalité et la disponibilité d'un service. Le MTRS peut, ou non, refléter la résolution finale d'un incident et/ou des systèmes impliqués.	
Démarrage à froid	Latence subie lors du déclenchement d'une fonction.	
Dépendance	Relation entre deux services, processus ou configurations qui dépendent l'un de l'autre pour fonctionner.	
Dépréciation	Fonctionnalité ou outil qui est mis(e) hors service, qui n'est plus utilisé(e) ou qui n'est plus mis(e) à jour.	

D

Deuxième niveau de support	Personnes qui sont incluses dans le processus de résolution/ remédiation et qui ont plus de capacité (temps, expérience, connaissances, ressources) pour résoudre le problème si les intervenants d'urgence ont besoin d'aide.	
Diagnostic (Diagnosis)	Processus visant à comprendre l'incident et ce qui l'a provoqué, et son résultat final.	
Diagnostic (Diagnostics)	« Symptômes » ou signes qui contribuent à un diagnostic lors d'un incident.	
Disponibilité	Qualité d'un service qui fonctionne comme prévu pour les utilisateurs pendant un temps de service convenu.	

E

Enregistrement d'un incident	Compilation des détails et du processus de résolution pour un incident donné.	
Enregistrement d'un problème	Document qui couvre tous les aspects d'un problème, sur l'ensemble de son cycle de vie.	

E

Environnement · **Environnement de développement** · **Environnement de tests** · **Environnement de production**	Type d'infrastructure informatique permettant de travailler sur un processus particulier. Il indique également les conditions extérieures qui affectent le processus concerné, ainsi que le contexte dans lequel elles l'affectent. · Infrastructure dans laquelle un service, une fonctionnalité, un processus, un élément de configuration, etc. est développé(e). · Infrastructure dans laquelle un service, une fonctionnalité, un processus, un élément de configuration, etc. est vérifié(e) pour s'assurer qu'il ou elle fonctionne comme prévu. Cet environnement est contrôlé plus étroitement pour reproduire l'environnement de production réel. · Infrastructure dans laquelle un service est fourni à un client. Les livrables dans cet environnement sont opérationnels, c'est pourquoi on parle aussi d'environnement de production.	
Équipe de réponse (également appelée équipe, tout court)	Unités opérationnelles dans une structure organisée, qui répondent aux alertes et aux incidents. Ces unités peuvent être regroupées par spécialisation technique, activité, services responsables, zone géographique, ou toute combinaison de ces éléments (ou d'autres).	

E

Erreur	Faute qui entraîne la défaillance totale d'un élément de configuration ou d'un service. Il peut s'agir d'une erreur de conception, de traitement ou d'une simple erreur humaine.	
Erreur connue	Bug ou problème préexistant, qui a été identifié dans un service et pour lequel une solution de contournement a déjà été implémentée.	
État **· Page d'état**	État actuel d'un service. · Page qui comprend l'état actuel d'un service, souvent accompagné de mises à jour de l'état de la société ou de l'équipe responsable.	
Événement	Changement d'état significatif pour un système ou un service. Peut survenir à la suite d'une action de l'utilisateur, ou être le signe d'une alerte ou d'un incident.	
Expert en la matière (SME)	Personne disposant de connaissances spécifiques sur un problème, un service, etc.	

F

Fatigue d'alerte	Situation dans laquelle les intervenants sont submergés par le volume ou la fréquence des alertes, et que leur capacité de réponse en souffre.	
Fermé	État final, qui indique que toutes les mesures nécessaires ont été prises.	
Fonctionnel	Capable de fonctionner comme prévu.	
Framework Cynefin	Structure décisionnelle qui a été adaptée aux processus de gestion des incidents afin d'aider les gestionnaires à identifier la façon dont ils perçoivent les situations et à organiser la réponse la plus efficace. Cynefin définit les incidents comme étant Simples, Compliqués, Complexes ou Chaotiques, puis décrit les réponses en fonction de cette assignation.	

G

Gestion des services informatiques (ITSM)	Tous les aspects des processus et procédures suivis pour fournir un service informatique aux clients. Cela concerne tous les aspects du cycle de vie du service, de la conception à la livraison.	

G

Gestionnaire/ Propriétaire de processus	Personne chargée de superviser les opérations en fonction des protocoles et des étapes nécessaires pour atteindre certains objectifs. Elle supervise l'ensemble du cycle de vie d'un processus, de la planification à l'exécution.	
Gravité	Mesure dans laquelle un service est affecté par un incident, y compris : durée de l'interruption, effort nécessaire pour y remédier et impact potentiel sur le business.	

H

Hotfix	Mise à jour appliquée à un logiciel afin de résoudre un problème ou un bug. Souvent utilisé pour résoudre spécifiquement un problème client.	
« Hot standby »	Option de reprise dans laquelle des actifs redondants fonctionnent simultanément pour assurer la continuité d'un service informatique en cas de défaillance.	

I

Impact	Mesure du coût, financier ou en termes de réputation, lié à une interruption de service, un incident ou un changement.	
Incident **· Réponse aux incidents** **· Gestion des incidents**	Défaillance imprévue, interruption de service ou réduction de la qualité de service attendue, qui a souvent un impact sur les besoins du business. · Réponse apportée à un incident, souvent planifiée en prévision de celui-ci. Des méthodes et des protocoles sont établis pour être mis en œuvre, et des personnes sont désignées pour agir en cas d'incident. · Processus de planification, de surveillance et d'alerte, de maîtrise, de résolution et d'analyse des incidents.	
Indicateurs clés de performance (KPI)	Mesures individuelles du succès d'un service, ou encore d'un processus ou d'une configuration informatique. Ces KPI sont décidés à l'avance pour établir des seuils d'alerte ou des rapports de base sur la réalisation des objectifs.	
Indicateurs de niveau de service	Métriques réelles qui représentent la fiabilité d'un service.	

I

Inforensique **· Investigation**	Investigation programmatique sur un système informatique dans le but d'identifier les incidents. · Collecte des éléments scientifiques et des preuves qui indiquent la cause d'un incident.	
Information Technology Infrastructure Library (ITIL)	Ensemble de pratiques largement acceptées, qui visent à aider les entreprises à faire en sorte que leurs services informatiques correspondent directement à leurs besoins et à leurs objectifs business.	
Ingénieur chargé de la fiabilité du site (SRE)	Personnes dont l'objectif est notamment d'automatiser les tâches manuelles, de gérer les SLO, de partager des outils avec les développeurs pour comprendre les services de leur organisation et de s'impliquer fortement dans les processus de résolution/remédiation des incidents.	
Interruption projetée du service (PSO)	Document qui décrit comment la maintenance ou les tests futurs affecteront les niveaux de service normaux.	

I

Intervalle moyen entre les défaillances (MTBF)	Mesure de la durée moyenne qui s'écoule à partir du moment où un service informatique commence à fonctionner jusqu'à sa prochaine défaillance. Ces analyses sont utiles pour les rapports et sont mesurées à partir du moment où le service est rétabli après une défaillance jusqu'à la prochaine défaillance.	
Intervalle moyen entre les incidents de service (MTBSI)	Mesure du temps moyen entre les interruptions de service qui sont classées comme des incidents, des indisponibilités du service ou des non-respects de la qualité attendue.	
Intervenant en cas d'incident	Personnes et/ou équipes responsables de l'investigation et de la résolution/remédiation d'un incident.	

Jargon des astreintes

Atténuation des incidents	Mesures initiales prises par les intervenants d'urgence dans le but de déployer des efforts de résolution/remédiation avant qu'une investigation complète n'ait été menée sur l'incident.	

Jargon des astreintes

Planning d'astreinte	Organisation et assignation des responsabilités afin de définir les intervenants informatiques chargés de répondre aux problèmes pendant une période déterminée.	
Planning de type « Follow the Sun »	Méthode de support client ou de gestion des incidents qui s'appuie sur des rotations d'astreinte sur plusieurs fuseaux horaires pour assurer une couverture 24 h/24 et 7 j/7.	
Premier niveau de support	Intervenant supposé réagir en premier à un incident. Il s'agit souvent l'ingénieur de support qui est d'astreinte.	
Remontée (ou « Escalade » [ITIL]) **· Fonctionnelle** **· Hiérarchique**	Méthode utilisée pour informer les intervenants d'un incident ou d'une alerte selon un ordre et un calendrier préétablis. · Méthode de remontée dans laquelle l'alerte ou l'incident est transféré(e) à une personne ayant plus d'expertise en assistance. · Méthode de remontée dans laquelle l'alerte ou l'incident est transféré(e) à une personne plus expérimentée pour obtenir une assistance.	

Jargon des astreintes

Rotation des astreintes	Passage de témoin d'un intervenant informatique à un autre pour répondre aux problèmes pendant une période donnée. Les rotations des astreintes sont des composantes des plannings d'astreinte.	

J

Journaux	Consignation de tous les événements liés à un service ou une application. Données transférées, heures et dates, incidents, changements, erreurs, etc.	

L

Latence	Retard subi lors du transfert de données.	

M

Maintenabilité	Propriété d'un service qui décrit la facilité avec laquelle les changements peuvent être appliqués avec succès dans un délai souhaité.	

M

Meilleure pratique **· Bonne pratique**	Les meilleures pratiques sont généralement considérées comme le « meilleur » moyen pour le secteur de mener à bien une tâche. Cependant, étant donné que la technologie est en constante évolution et que les environnements sont propres à chaque organisation, ce terme est souvent considéré comme trop restrictif par nature, car il impose aux méthodes une norme quasi impossible à atteindre. · Le terme « bonne pratique » est souvent utilisé à la place de « meilleure pratique », car il offre une plus grande flexibilité dans son application en contrebalançant les différentes interprétations d'une entreprise à l'autre, les innovations constantes liées aux nouvelles technologies et la créativité, afin de créer d'autres bonnes pratiques au lieu de limiter la résolution des problèmes à une seule norme ultime.	
Menace	Événement potentiel qui pourrait nuire à un service par le biais d'une vulnérabilité.	
Métriques en tension	Données qui, lorsqu'un ensemble ou un point est modifié, affectent négativement d'autres points de données.	

M

Métriques entrantes/ sortantes	Données entrantes et sortantes. Dans une entreprise, ces métriques constituent souvent la base sur laquelle reposent les objectifs. Les métriques entrantes sont des comportements contrôlés par une entreprise afin d'atteindre des métriques sortantes spécifiques.	
Mise en production · **Gestion des mises en production**	Changement déployé auprès des utilisateurs. Il peut s'agir de n'importe quel élément de configuration. · Planification, conception, tests, programmation, dépannage et déploiement des changements. Il s'agit, dans les grandes lignes, de la supervision de tout le cycle de vie d'une mise en production.	
Modèle/Modélisation	Représentation d'un système, d'un service, d'une application, etc.	

N

Notification	Message délivré sous une forme quelconque (mobile, e-mail, etc.).	

O

Objectifs de niveau de service (SLO)	Objectifs visés pour la fiabilité d'un service.	

O

Observabilité	Propriété d'un système désignant le volume de données qu'il est possible de déduire des résultats avec précision.	
Observation technique (TO)	Technique utilisée par les professionnels de l'informatique spécialisés dans la surveillance et les services informatiques pour comprendre la disponibilité, les problèmes et les domaines d'amélioration possibles.	
Orchestration de la réponse aux incidents	Offre Opsgenie qui comprend des composants et des fonctionnalités que les utilisateurs peuvent utiliser lors de la résolution d'incidents pour aider les organisations à identifier rapidement et efficacement les problèmes, à avertir les bonnes personnes, à faciliter la communication entre les unités business et à collaborer.	

P

Parties prenantes et observateurs des incidents	Personnes qui doivent être tenues au courant d'un incident et qui peuvent influencer sa résolution, mais ne sont pas des intervenants actifs.	
Performance	Mesure de ce qui est obtenu par une personne, un système, un service ou un élément de configuration, etc. liés à l'informatique.	

P

Périmètre	Ampleur d'un problème, d'une solution, d'un projet, d'une capacité, etc.	
Période d'interruption	Intervalle pendant lequel un service ou une partie d'un service ne fonctionne pas comme prévu.	
Point de défaillance unique (SPOF)	Seule variable dont dépend un incident pour fonctionner, comme un élément de configuration essentiel ou le personnel impliqué.	
Prendre connaissance	Action d'alerte qui informe les autres destinataires de l'alerte que celle-ci a été vue et qu'elle est en cours de traitement.	
Priorité	Transmet la gravité, l'urgence et/ou l'impact potentiel en assignant un niveau à une alerte/un incident, afin que les intervenants puissent réagir en conséquence.	

R

Rapport d'exception	Compte rendu des dépassements des seuils définis pour les indicateurs clés de performance (KPI), généralement de manière négative.	

R

Reprise **· Objectif de point de reprise (RPO)** **· Objectif de temps de reprise (RTO)**	Processus visant à rétablir la fonctionnalité et l'intégrité d'un service, système, etc. à sa base de référence. · Quantité maximale de données qui seront perdues pendant la restauration par rapport au temps d'indisponibilité. · Durée maximale tolérée pour une interruption de service.	
Reprise graduelle	[Voir « Cold standby »]	
Reprise immédiate	Option de reprise qui utilise la redondance, ou le miroitage, pour restaurer les systèmes en cas de défaillance. Voir [« Hot standby »].	
Reprise intermédiaire	Option de reprise graduelle qui comporte certains composants fixes, mais des opérations de restauration et de configuration devront être effectuées pour rétablir les systèmes, ce qui peut prendre plus de 24 heures. Voir [« Reprise à chaud »].	
Résilience	Capacité d'un système ou d'un service informatique à résister à une défaillance et à se rétablir dans un délai souhaité.	
Résolution	Action ou processus consistant à prendre une mesure pour ramener les systèmes à un fonctionnement normal.	

R

Responsable de la communication	Personne qui, lors d'un incident, est chargée d'orchestrer la collaboration et de relayer les informations pertinentes entre les équipes.	
Responsable des incidents	Personne qui détient le contrôle ultime et la capacité de prise de décision lors d'un incident.	
Responsable des opérations	Personne chargée de superviser les opérations quotidiennes et de s'assurer que les services fonctionnent comme prévu. Lors d'incidents, les ingénieurs informent le responsable des opérations grâce à des mises à jour sur une résolution.	
Résultat	Résultat d'un événement, d'un processus ou d'un changement informatique. Les résultats peuvent être abordés à la fois comme ce qui est prévu et comme le résultat réel.	
Retour arrière	Action consistant à restaurer un service à un état ou une base de référence fiable antérieure, afin de fournir la fonctionnalité attendue aux utilisateurs si une mise à jour ou une mise en production n'a pas réussi.	

R

Revue post-action (AAR)	Analyse qui a lieu après un événement et fournit des détails spécifiques : description de l'événement, cause et domaines à améliorer pour éviter qu'il ne se reproduise. Les revues post-action sont souvent connues sous le nom de rapports d'analyse post-mortem ou post-incident.	
Risque **· Évaluation** **· Gestion**	Événement susceptible de nuire à un actif du business précieux. · Processus visant à identifier la valeur d'un actif, les menaces potentielles pesant sur cet actif et leur impact potentiel, ainsi que la vulnérabilité d'un actif à ces menaces. · Processus visant à traiter les menaces en les identifiant, puis en les contrôlant en fonction de l'actif sur lequel elles peuvent avoir un impact.	
Runbooks	Procédures et processus détaillés, exécutés par un administrateur système ou un centre d'opérations réseau. Les runbooks peuvent être créés sous forme numérique ou physique.	

S

Salle de contrôle	Lieu physique où a lieu la surveillance des services informatiques.	

S

Secrétaire	Personne chargée de documenter l'incident et les processus pendant la résolution/ remédiation.	
Service (axé informatique) **· Services « disponibles en continu »** **· Changement de service**	Offre faite aux clients qui procure une valeur ajoutée et résout la difficulté qu'ils rencontrent. · Service qui est censé fonctionner en continu, quel que soit l'objectif visé par l'utilisateur. · Altérations apportées à un service, telles que les mises à jour, les corrections ou la dépréciation d'une fonctionnalité.	
Service de base	Service qui assure une fonction centrale pour les utilisateurs et/ou les clients.	
Service de soutien	Service requis afin qu'un service de base fonctionne et soit disponible pour les clients, mais qui n'est pas directement offert aux clients.	
Service visible par le business	Services que les clients utilisent et avec lesquels ils interagissent.	
Seuil	Point identifié pour lequel des alertes sont générées lors de son franchissement.	

S

Solution de contournement	Méthode efficace pour implémenter une correction jusqu'au point où la majeure partie des fonctionnalités sont encore disponibles, mais où l'incident sous-jacent n'est pas encore résolu.	
Solution de contournement manuelle	Solution exécutée manuellement, c'est-à-dire pas de façon automatique.	
Spécification	Registre officiel des exigences propres à un élément de configuration informatique. Aux fins de l'adhésion au code de pratiques et de normes.	
Stack technique	Langages de programmation, logiciels et composants qui constituent une application. Une stack technique comporte deux parties : le front-end (face au client) et le back-end (face au développeur).	
Surveillance	Processus répété de vérification d'un service ou d'un processus pour s'assurer qu'il fonctionne comme prévu, et pour détecter les événements indiquant une interruption ou un changement d'état.	
Surveillance active	Méthode permettant de comprendre l'état actuel, ou les changements d'état, d'un service par le biais de contrôles réguliers.	

S

Surveillance passive	Processus de surveillance (vérification de la fonctionnalité d'un service) dans le cadre duquel un problème ne peut être indiqué que par le biais d'une alerte ou d'une notification.	
Surveillance réactive	Processus de surveillance (vérification de la fonctionnalité d'un service) qui est uniquement effectué en cas d'erreur ou d'incident.	
Système de gestion de la qualité (QMS)	Cadre mis en place pour garantir et s'assurer qu'une organisation atteint les objectifs et les résultats escomptés.	
Système de gestion des configurations (CMS)	Système organisant toutes les informations utilisées pour apporter un support aux différents services ou produits qu'une entreprise utilise et fournit. Tient à jour les informations opérationnelles pour les éléments de configuration, ainsi que la conception, la consignation des incidents et toute autre donnée pertinente.	

T

Tableau de bord	Visualisation simple des systèmes, des alertes et des incidents conçue pour organiser la présentation d'informations provenant d'outils disparates, avec des informations contextuelles fournies dans un format propre et précis.	
Tableau SLAM	Tableau de surveillance des accords sur les niveaux de service qui consigne l'avancement et des données sur les objectifs de niveau de service.	
Temps de guerre	Période pendant laquelle un incident s'est produit et a fait l'objet d'un triage et d'un rattrapage.	
Temps de paix	Période pendant laquelle les services et les opérations fonctionnent comme prévu, sans aucune interruption.	
Temps de réponse	Délai nécessaire afin d'identifier et de prendre les premières mesures pour tout événement unique qui justifie une réponse.	
Temps de service convenu (AST)	Période pendant laquelle un service est disponible et remplit la fonction attendue.	

T

Temps d'indisponibilité planifié	Période pendant laquelle un service informatique est, de manière attendue et intentionnelle, indisponible à des fins de maintenance ou de mise à jour.	
Temps d'indisponibilité/ Interruption	Période ou situation au cours de laquelle un service ne fonctionne pas ou n'est pas disponible comme prévu.	
Tolérance aux pannes	Capacité d'un service de continuer à fonctionner même après une défaillance d'un élément de configuration ou d'un composant.	
Triage	Processus visant à identifier toutes les parties d'un incident ou d'un problème, et à planifier le processus de résolution/ remédiation.	

V

Variance	Incohérences entre les valeurs.	
Vérification	Activité qui confirme qu'un incident s'est produit ou a été résolu selon les normes prévues.	

Conclusion

Une gestion rapide et efficace des incidents est le cœur même des opérations informatiques de toute organisation.

Les coûts en jeu étant élevés, on comprend aisément pourquoi les équipes les plus performantes adoptent une posture digne des temps de « guerre » lors d'un incident, mais aussi pourquoi le langage en temps de guerre doit être spécifique, direct et exploitable afin de communiquer clairement pour identifier un problème, ainsi que les mesures à prendre et par qui.

Nos plateformes technologiques deviennent infiniment plus complexes et imbriquées. C'est pourquoi la fréquence et la gravité des incidents ne cesseront de croître. En se concentrant sur le langage adopté lors d'un incident, les équipes peuvent mieux collaborer pour trouver la résolution la plus rapide possible.

Pour plus d'informations sur la gestion moderne des incidents, consultez la bibliothèque de ressources d'Opsgenie : https://www.opsgenie.com/resource-library

À PROPOS DE L'AUTEUR

Elizabeth Riezinger

Elizabeth Riezinger est rédactrice technique pour Opsgenie (acquis par Atlassian). Elle travaille en collaboration avec l'équipe d'ingénieurs pour rédiger et éditer la documentation, l'optimiser grâce à des visuels pertinents et mener à bien la stratégie de contenu dans la documentation et les ressources. Sa compréhension des principes DevOps lui a permis de contribuer à la réalisation de nombreux projets qui soutiennent des organisations en pleine modernisation de leurs processus de gestion des incidents.

ATLASSIAN