Engineer

Analyse post-incident

Compte rendu d’incident pour éviter qu’il se reproduise

Ce que c’est

Une analyse post-incident, ou postmortem, est le compte rendu qu’une équipe rédige après un incident : ce qui s’est passé, ce que cela a coûté, les mesures prises pour l’arrêter, ses causes et les changements prévus pour éviter qu’il se reproduise de la même façon. Le mot postmortem s’écrit aussi post-mortem, avec un trait d’union ; le sens est identique. Le livre Site Reliability Engineering de Google le définit en ces termes : un compte rendu qui relie un incident et ses conséquences à la réponse apportée, aux causes et au travail nécessaire pour éviter une récidive.

Le livre donne trois objectifs à l’exercice : documenter l’incident, comprendre toutes les causes profondes qui y ont contribué plutôt que la première trouvée, et mettre en place des mesures préventives réellement efficaces. Le pluriel compte. Quelle que soit la taille du système, un incident a rarement une cause unique. Une analyse qui s’arrête à la première explication plausible tend à corriger le déclencheur tout en laissant en place les conditions qui lui ont permis de faire des dégâts.

Ce qui distingue cette pratique d’un rapport ordinaire, c’est l’absence de recherche de coupable. Une analyse post-incident sans blâme recherche les causes contributives sans accuser une personne ou une équipe de s’être mal comportée. Elle part du principe que les personnes concernées étaient bien intentionnées et ont décidé avec les informations dont elles disposaient à ce moment-là. Le livre SRE rattache cette idée à la santé et à l’aviation, deux domaines où une erreur peut être fatale et où chaque erreur est considérée comme une occasion de renforcer le système. Le raisonnement est pratique plutôt que bienveillant : on ne peut pas appliquer un correctif à une personne, mais on peut le faire à un système ou à un processus.

On ne rédige pas une analyse post-incident au moindre accroc, car cela prend du temps. Le livre énumère les déclencheurs habituels, dont chaque équipe adapte les seuils à ses besoins :

- une indisponibilité ou une dégradation visible par les utilisateurs, au-delà d'une limite convenue ;
- toute perte de données ;
- une intervention nécessaire de l'ingénieur d'astreinte, par exemple pour annuler une mise en production ou réorienter le trafic ;
- un délai de résolution supérieur à une limite convenue ;
- une défaillance de la supervision, ce qui signifie généralement qu'une personne a découvert le problème en premier.

Les critères sont convenus avant qu'une panne survienne, pour ne pas avoir à débattre en pleine interruption de service de leur applicabilité. Toute partie prenante peut aussi demander une analyse d'un événement qui sort de ces critères.

Utilisez le concept pour prendre une décision

Utilisez « Qu'est-ce qu'une analyse post-incident ? » pour éclairer une décision réelle. Nous pouvons vous aider à relier ce concept au système que vous construisez ou achetez. Une supervision et des alertes qui signalent les incidents tant qu'ils restent mineurs, avec les chiffres qui montrent à quelle fréquence ils le restent.

Découvrir nos prestations Contactez-nous →

Vérifiez les hypothèses derrière le terme

Appuyez-vous sur l'explication et les réalisations liées pour formuler les questions de votre projet. Nous pouvons examiner les hypothèses avec vous avant le choix d'un outil. Premier tableau de bord d'observabilité — première vue de l'entreprise sur ses propres systèmes

Premier tableau de bord d'observabilité Contactez-nous →

Pourquoi c'est important

Un incident corrigé mais non documenté risque de se reproduire. Le SRE Workbook examine une analyse publiée quatre mois après l'incident qu'elle décrivait ; entre-temps, le même incident s'était reproduit, et l'équipe avait dû reconstituer ce qu'elle avait appris la première fois. Un compte rendu rédigé rapidement et conservé là où chacun peut le retrouver transforme le mauvais après-midi d'une équipe en connaissances utiles à toute l'organisation.

Le compte rendu oblige aussi à donner une existence au suivi. Ben Treynor Sloss, cité dans le Workbook, le dit sans détour : une analyse post-incident n'apporte rien aux utilisateurs si l'équipe ne donne pas suite à ses conclusions. Google exige

donc que chaque analyse faisant suite à une interruption affectant les utilisateurs comporte au moins un ticket de suivi à l'un des deux niveaux de priorité les plus élevés. L'analyse sert à justifier ce travail, preuves à l'appui, et permet d'en vérifier l'avancement par la suite.

L'absence de blâme rend les éléments recueillis dignes de confiance. Là où les erreurs valent de l'humiliation à leurs auteurs, observe le livre SRE, les personnes cessent de signaler les problèmes. Le Workbook ajoute qu'elles peuvent cacher précisément les faits nécessaires pour éviter une récidive. Une culture sans blâme obtient la chronologie complète, y compris la commande lancée par erreur, parce que personne n'est puni pour l'avoir racontée. Le livre va plus loin : une équipe ou une personne qui rédige beaucoup d'analyses post-incident ne doit pas être considérée comme un problème, puisque l'autre possibilité est que des incidents restent sans compte rendu.

Réunies, les analyses post-incident constituent un jeu de données. Dès que chacune porte les mêmes métadonnées, l'organisation peut suivre des tendances comme le délai de détection, le délai de résolution et l'étendue des incidents, et voir si le travail de fiabilité porte ses fruits. Les mêmes comptes rendus servent à la formation : Google rejoue d'anciennes analyses sous forme de jeux de rôle pour les nouveaux ingénieurs, organise des clubs de lecture et publie une lettre d'information avec une analyse du mois.

À quoi cela ressemble en pratique

Le livre SRE publie un exemple complet en annexe D, consacré à un service de recherche fictif tombé en panne pendant 66 minutes sous un afflux soudain de trafic. Ses rubriques constituent un bon point de départ : état, résumé, impact, causes profondes, déclencheur, résolution, détection, actions, enseignements — ce qui a bien fonctionné, ce qui a mal fonctionné, les circonstances favorables — et chronologie en UTC. La chronologie distingue quatre moments : le début de la panne, la déclaration de l'incident, la fin de la panne et la clôture formelle de l'incident. Ce sont des moments différents, et les intervalles qui les séparent sont souvent les plus riches d'enseignements.

Voici une analyse reprenant cette structure pour un incident inventé, réduite à ce qui tient sur un écran :

```
Analyse post-incident : échecs à l'encaissement après un changement de délai
État :       définitif, relu
Responsable : ingénieur d'astreinte, avec le responsable de l'incident
Résumé :     environ un tiers des demandes d'encaissement échouent durant 31 min
Impact :     environ 4 100 encaissements échoués, aucune donnée perdue ;
             budget d'erreur d'encaissement de 28 jours épuisé en une soirée
Causes profondes : délai de paiement réduit de 10 s à 1 s, changement relu comme
             « configuration seule » ; aucun essai à charge de pointe avant
             la mise en production
Déclencheur : au pic du soir, le prestataire de paiement met plus de 1 s
Détection :  l'alerte sur le taux d'erreur appelle l'astreinte 6 min après
             la première erreur
Résolution : retour arrière du changement ; fin des échecs 4 min plus tard

Actions
  Type       Priorité  Responsable       Terminé quand
  prévenir   P1        resp. plateforme  chaque changement de configuration
                                         passe le test de charge
  détecter   P1        resp. astreinte   l'alerte signale les délais de paiement
                                         dépassés
  atténuer   P2        resp. encaissement retour arrière de configuration
                                         en une seule étape
  procédure  P2        resp. incident    les changements de configuration
                                         figurent au journal des déploiements

Enseignements
  Réussite :  le retour arrière a fonctionné du premier coup
  Échec :     un changement de délai n'a pas été traité comme du code
  Chance :    le pic a été court ; un jour de soldes l'aurait triplé

Chronologie (UTC)
  18:02  changement fusionné et déployé
  18:40  pic de trafic ; premiers échecs d'encaissement     début de la panne
  18:46  l'alerte sur le taux d'erreur appelle l'astreinte
  18:52  incident déclaré, responsable désigné             début de l'incident
  19:07  changement de délai identifié, retour arrière lancé
  19:11  fin des échecs                                    fin de la panne
  19:41  trente minutes à taux d'erreur normal             fin de l'incident
```

Remarquez ce qui manque : aucun nom de personne dans les causes, aucune action demandant à quelqu'un de faire plus attention. Chaque action a un responsable unique, une priorité et un état final qu'une autre personne peut vérifier. La plupart des éléments de départ n'ont pas non plus à être reconstitués de mémoire. Dans le chapitre du livre SRE consacré à la gestion des incidents, la personne qui dirige l'incident tient un document mis à jour pendant son déroulement, à conserver pour l'analyse ultérieure. Le Workbook décrit aussi des outils qui renseignent automatiquement les rôles, la chronologie et les services touchés.

Sur ce site, le compte rendu de l'incident des tampons d'événements sous macOS, daté de septembre 2026, reprend une grande partie de la structure d'une analyse post-incident. Il distingue des rapports de diagnostic faisant état de 111 Go de pages compressées sur une machine de 36 Go d'un échantillon distinct montrant une croissance de l'empreinte mémoire d'environ 41 Mo par seconde. Il identifie un flux principal d'événements non borné et des événements de journalisation copiés vers des abonnés qui ne les utilisaient pas, puis borne les tampons, filtre les abonnements par type d'événement et attribue un budget de débit à la journalisation. Une comparaison sur un cycle complet de tests relève une baisse de 610 996 à 1 411 lignes de journal du cœur. Des contrôles d'architecture et des tests de budget protègent la conception, tandis que le compte rendu précise ce que les éléments disponibles ne permettent pas d'établir : une mesure mémoire après correction ou un benchmark en production. Des dépassements de délai à l'arrêt ont nécessité leur propre correction, et le budget permet délibérément d'abandonner des événements de diagnostic répétitifs. Le récit des trois verrous sur la porte, dont aucun n'était verrouillé décrit une revue plutôt qu'une panne, mais aboutit là où une bonne analyse post-incident devrait mener : les trois correctifs étaient modestes, et le travail a produit deux règles qui régissent désormais le dépôt, afin de détecter toute cette catégorie de défaillances plutôt que les trois occurrences.

Où les problèmes surviennent

Le document désigne un coupable. Une analyse qui attribue toute la responsabilité à une personne ou parle de son « ignorance doublée de négligence » enseigne aux autres à se taire la prochaine fois. Écrivez ce qui s'est passé et ce que la personne savait alors, sans porter de jugement sur ce qu'elle est, et restez factuel : le Workbook considère les formulations dramatiques et les points d'exclamation comme des distractions qui détournent l'attention des faits.

Les actions demandent aux humains de redoubler d'efforts. Des consignes comme « faire plus attention » et « améliorer le guide d'exploitation » ne permettent pas de clôturer une action, et changer les comportements est moins fiable que changer le système. Donnez à chaque action un type — prévenir, atténuer, détecter —, un responsable unique, une priorité et un état final vérifiable, par exemple une alerte qui se déclenche au-delà d'un seuil indiqué. Ouvrez pour chacune un ticket dans l'outil de suivi que l'équipe consulte déjà.

La recherche des causes profondes s'arrête au déclencheur. « Un changement de configuration a provoqué la panne » désigne le déclencheur. Les causes profondes expliquent pourquoi ce changement a pu faire autant de dégâts : pourquoi la revue ne l'a pas repéré, pourquoi aucun test ne l'a détecté, pourquoi l'alerte est arrivée tard. Gardez deux rubriques distinctes, comme dans l'exemple du livre SRE.

L'impact se résume à un haussement d'épaules. Si la durée est le seul chiffre du document, personne ne peut savoir si le correctif a fonctionné. Estimez le nombre d'utilisateurs touchés, les requêtes perdues et le budget d'erreur consommé : selon le Workbook, une estimation bien informée vaut mieux que l'absence totale de données.

Quatre personnes en sont responsables, donc personne ne l'est. L'analyse doit avoir un responsable unique, interlocuteur pour sa rédaction et pour le suivi jusqu'à son terme, avec l'aide des autres. Il en va de même pour chaque action.

Le document est rédigé tard, ou personne ne le lit. Les souvenirs s'estompent en quelques jours, et un document diffusé des mois plus tard arrive après la récidive. Le bon exemple du Workbook a été diffusé largement dans la semaine suivant la clôture de l'incident. Faites-le aussi relire : « Une analyse post-incident non relue aurait tout aussi bien pu ne jamais exister », selon le livre SRE. Organisez des séances de revue régulières, puis conservez le résultat dans des archives consultables par recherche.

Les actions ne sont jamais clôturées. Quand le même incident revient, vérifiez si les actions prennent trop de temps et si les nouvelles fonctionnalités passent toujours avant les correctifs de fiabilité. Suivez les clôtures plutôt que les rédactions : Google organise deux fois par an des semaines FixIt et récompense les ingénieurs qui clôturent le plus d'actions issues d'analyses post-incident.

Pour aller plus loin

- Culture de l'analyse post-incident : apprendre des échecs — chapitre 15 du livre Site Reliability Engineering de Google : déclencheurs, absence de blâme, revue et culture associée.
- Culture de l'analyse post-incident : apprendre des échecs — le chapitre du SRE Workbook, avec une mauvaise et une bonne analyse du même incident et les raisons qui les distinguent.

- Exemple d’analyse post-incident — une analyse complète d’une panne fictive, avec actions, enseignements et chronologie.
- Gérer les incidents — chapitre 14 du livre SRE : la direction de l’incident, le document tenu à jour et les passages de relais sur lesquels l’analyse s’appuie ensuite.

Glossaire

Choisissez selon vos contraintes réelles

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Rendez la terminologie concrète

Demandez comment « Qu’est-ce qu’une analyse post-incident ? » s'applique à votre organisation. Un exemple concret tiré de votre système actuel suffit pour engager la discussion.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/glossary/postmortem/