Engineer

Постмортем

письмовий розбір інциденту, його причин і подальших дій

Що це таке

Постмортем — це письмовий розбір, який команда складає після інциденту: що сталося, чого це коштувало, що зробили, щоб це зупинити, чому це сталося і що зміниться, аби те саме не повторилося так само. Слово прийшло з англійської (postmortem, також post-mortem через дефіс), і українські команди здебільшого так його й уживають, поряд з описовим «розбір інциденту». Книга Google Site Reliability Engineering визначає його саме так: письмовий запис про інцидент, його наслідки, дії, якими його пом'якшили або усунули, першопричини та подальші заходи, що мають запобігти повторенню.

Книга ставить перед цією практикою три цілі: задокументувати інцидент, зрозуміти всі причини, що до нього призвели, а не лише першу знайдену, і запровадити запобіжні заходи, які справді працюють. Множина тут важлива. У системах будь-якого помітного розміру інцидент рідко має одну причину, і розбір, що зупиняється на першому правдоподібному поясненні, зазвичай виправляє тригер і залишає умови, які дали тригерові змогу завдати шкоди.

Від звичайного звіту цю практику відрізняє те, що вона не шукає винних (англійською blameless). Такий постмортем з'ясовує причини, не звинувачуючи жодну людину чи команду в поганій поведінці, і виходить з того, що всі учасники діяли з добрими намірами й ухвалювали рішення на основі інформації, яку мали на той момент. Книга SRE виводить цю ідею з охорони здоров'я та авіації — галузей, де помилка може коштувати життя і де кожну помилку розглядають як нагоду зробити систему міцнішою. Аргумент тут практичний, а не етичний: людину патчем не виправиш, а систему чи процес — можна.

Постмортем пишуть не через кожну дрібницю, бо це забирає час. Книга називає типові тригери, а кожна команда підлаштовує пороги під себе:

- простій або погіршення сервісу, помітні користувачам, понад узгоджену межу;
- втрата даних будь-якого виду;
- втручання чергового інженера, наприклад відкат релізу чи перенаправлення трафіку;
- час усунення понад узгоджену межу;
- збій моніторингу, що зазвичай означає: проблему першою помітила людина.

Критерії узгоджують заздалегідь, поки нічого не зламалося, щоб посеред збою ніхто не сперечався, чи рахується саме цей випадок, а будь-яка зацікавлена сторона може попросити постмортем і тоді, коли подія під критерії не підпадає.

Застосуйте поняття до рішення

Застосуйте «Що таке постмортем?» до конкретного рішення. Ми можемо пов'язати поняття із системою, яку ви створюєте або купуєте. Моніторинг і сповіщення, які попереджають, поки збій ще малий, і цифри, що показують, як часто так і залишається.

Переглянути наші послуги Зв'язатися з нами →

Перевірте припущення за терміном

Використайте пояснення та пов'язані роботи, щоб сформулювати запитання для проєкту. Ми можемо перевірити припущення разом до вибору інструмента. Запустила перший дашборд спостережуваності — перший огляд власних систем компанії

Запустила перший дашборд спостережуваності Зв'язатися з нами →

Чому це важливо

Інцидент, який виправили, але не описали, легко повторюється. SRE Workbook розбирає постмортем, опублікований через чотири місяці після інциденту; за цей час той самий інцидент стався знову, і команді довелося заново відтворювати те, що вона з’ясувала ще першого разу. Розбір, написаний вчасно й збережений там, де його можна знайти, перетворює невдалий день однієї команди на знання, яким може скористатися вся організація.

Документ також змушує подальші дії з’явитися. Бен Трейнор Слосс, якого цитує Workbook, каже прямо: для користувачів постмортем без подальших дій нічим не відрізняється від відсутності постмортему. Тому Google вимагає, щоб кожен постмортем після збою, який зачепив користувачів, мав

щонайменше одну задачу в трекері з одним із двох найвищих пріоритетів. Постмортем — це місце, де аргумент на користь цієї роботи викладають із доказами і де згодом можна перевірити, чи її виконано.

Відмова від пошуку винних робить свідчення достовірними. Там, де людей соромлять за помилки, зауважує книга SRE, вони перестають розповідати про проблеми, а Workbook додає, що вони можуть приховати саме ті факти, які потрібні, щоб запобігти повторенню. Культура без пошуку винних отримує повну хронологію, разом із командою, яку хтось помилково запустив, бо за розповідь про неї нікого не карають. Книга йде ще далі: команду чи людину, яка пише багато постмортемів, не слід вважати проблемою, адже альтернатива — інциденти, про які ніхто не пише.

Разом постмортеми стають набором даних. Коли кожен має однакові метадані, організація може стежити за тенденціями — часом до виявлення, часом до усунення, тим, наскільки широко поширився інцидент, — і бачити, чи окупається робота над надійністю. Ті самі документи слугують і для навчання: Google розігрує старі постмортеми як рольові ігри для нових інженерів, проводить читацькі клуби й розсилає бюлетень із постмортемом місяця.

Як це виглядає на практиці

Книга SRE наводить повний приклад у додатку D, написаний для вигаданого пошукового сервісу, який лежав 66 хвилин під раптовою хвилею трафіку. Його розділи — добра основа: статус, короткий виклад, наслідки, першопричини, тригер, усунення, виявлення, подальші дії, висновки (що вдалося, що пішло не так, де пощастило) і хронологія в UTC. Хронологія окремо позначає чотири моменти: коли почався збій, коли оголосили інцидент, коли збій закінчився і коли інцидент формально закрили. Це різні моменти, і саме в проміжках між ними зазвичай ховаються висновки.

Ось постмортем у такій формі для вигаданого інциденту, скорочений до одного екрана:

```
Постмортем: збої оплати після зміни тайм-ауту
Статус:        остаточний, розглянутий
Власник:       черговий інженер разом із керівником інциденту
Виклад:        оплата не проходила приблизно для третини запитів 31 хв
Наслідки:      приблизно 4 100 невдалих оплат, дані не втрачено;
```

```
                бюджет помилок оплати на 28 днів витрачено за один вечір
Першопричини:   тайм-аут до платіжного провайдера знижено з 10 с до 1 с
                у зміні, яку розглянули як «лише конфіг»; до релізу
                під піковим навантаженням її ніхто не перевіряв
Тригер:         вечірній пік сповільнив провайдера понад 1 с
Виявлення:      сповіщення про частку помилок викликало чергового
                через 6 хв після першої помилки
Усунення:       зміну відкочено; збої припинилися за 4 хв

Подальші дії
  Тип          Пріор.  Власник              Готово, коли
  запобігти    P1      керівник платформи   конфіг проходить тест навантаження
  виявити      P1      керівник чергувань   є сповіщення про тайм-аути оплати
  пом'якшити   P2      керівник оплати      відкат конфігу робиться за крок
  процес       P2      керівник інцидентів  зміни конфігу видно в журналі

Висновки
  Вдалося:      відкат спрацював з першої спроби
  Не вдалося:   зміну тайм-ауту не розглядали як зміну коду
  Пощастило:    пік був коротким; у день розпродажу він був би втричі більшим

Хронологія (UTC)
  18:02  зміну злито й розгорнуто
  18:40  пік трафіку; перші збої оплати            початок збою
  18:46  сповіщення про частку помилок викликає чергового
  18:52  оголошено інцидент, призначено керівника  початок інциденту
  19:07  знайдено зміну тайм-ауту, почато відкат
  19:11  збої припиняються                         кінець збою
  19:41  тридцять хвилин зі звичною часткою помилок   кінець інциденту
```

Зверніть увагу на те, чого тут немає: імен у причинах і подальших дій, які просять когось бути уважнішим. Кожна дія має одного власника, пріоритет і кінцевий стан, який може перевірити хтось інший. Більшість сирого матеріалу теж не доводиться відновлювати з пам’яті. Розділ книги SRE про керування інцидентами доручає керівникові інциденту вести живий документ, поки інцидент триває, і зберегти його для постмортему, а Workbook описує інструменти, які самі заповнюють ролі, хронологію та зачеплені сервіси.

На цьому сайті запис про інцидент із буфером подій у macOS, від вересня 2026 року, має більшість структурних рис постмортему. Він відокремлює діагностичні звіти про 111 ГБ стиснутих сторінок на машині з 36 ГБ від окремого заміру обсягу зайнятої пам’яті зі зростанням приблизно на 41 МБ за секунду. У ньому виявлено необмежений основний потік подій і події журналу, які копіювалися підписникам, що їх не використовували; після цього обмежено буфери, відфільтровано підписки за типом події та надано

журналюванню бюджет частоти записів. Порівняння повних тестових запусків фіксує скорочення 610 996 рядків журналу ядра програми до 1 411. Архітектурні перевірки й тести бюджетів перевіряють дотримання цієї схеми, а опис прямо вказує, чого докази не підтверджують: виміряного показника використання пам'яті після виправлення чи бенчмарку у виробничому середовищі. Окремі тайм-аути під час завершення роботи потребували власного виправлення, а бюджет навмисно дозволяє відкидати повторювані діагностичні події. Кейс три замки на дверях, і жоден не замкнений описує перевірку, а не збій, але закінчується там, де має закінчуватися добрий постмортем: три виправлення були дрібними, а підсумком роботи стали два правила, які тепер діють у репозиторії, щоб виявляти цілий клас вад, а не три окремі випадки.

Де виникають проблеми

Документ називає винного. Постмортем, де написано, що відповідальність лежить на одній людині, або де йдеться про її «недбале невігластво», вчить усіх інших наступного разу мовчати. Пишіть про те, що сталося і що людина знала на той момент, а не про те, яка вона, і тримайтеся фактів; Workbook зазначає, що емоційні формулювання та знаки оклику відволікають від суті.

Подальші дії просять людей старатися краще. «Бути уважнішим» і «покращити інструкцію для чергових» неможливо закрити, а змінювати поведінку менш надійно, ніж змінювати систему. Дайте кожному пункту тип (запобігти, пом'якшити, виявити), одного власника, пріоритет і кінцевий стан, який можна перевірити, — скажімо, сповіщення, що спрацьовує понад названий поріг, — і заведіть задачу для кожного пункту в трекері, за яким команда вже стежить.

Першопричина зупиняється на тригері. «Зміна конфігурації спричинила збій» називає тригер. Першопричини — це те, чому зміна змогла завдати стільки шкоди: чому її пропустили на рев'ю, чому жоден тест її не впіймав, чому сповіщення прийшло запізно. Тримайте ці два розділи окремо, як це зроблено в прикладі з книги SRE.

Наслідки описано знизуванням плечей. Якщо єдине число в документі — тривалість, ніхто не скаже, чи спрацювало виправлення. Оцініть кількість зачеплених користувачів, утрачених запитів і витрачений бюджет помилок; порада Workbook — добре обґрунтована оцінка краща, ніж жодних даних узагалі.

Ним володіють четверо, тож не володіє ніхто. Постмортему потрібен один власник — єдина контактна особа і для написання, і для того, щоб довести подальші дії до кінця, а інші допомагають. Те саме стосується кожного окремого пункту.

Його пишуть запізно, або його ніхто не читає. Пам'ять тьмяніє за кілька днів, а документ, розісланий через кілька місяців, приходить уже після наступного повторення. Добрий приклад у Workbook розіслали широкому колу менше ніж через тиждень після закриття інциденту. І розглядайте його: «Нерозглянутий постмортем міг би й зовсім не існувати», як пише книга SRE. Проводьте регулярні зустрічі для розгляду, а результат зберігайте в архіві з пошуком.

Подальші дії так і не закриваються. Коли той самий інцидент повертається знову й знову, перевірте, чи не надто довго виконуються подальші дії і чи не перемагає раз у раз робота над новими функціями виправлення надійності. Вимірюйте закриття, а не авторство: Google двічі на рік проводить тижні FixIt і відзначає інженерів, які закрили найбільше пунктів із постмортемів.

Що почитати далі

- Postmortem Culture: Learning from Failure — розділ 15 книги Google Site Reliability Engineering: тригери, відмова від пошуку винних, розгляд і культура навколо всього цього.
- Postmortem Culture: Learning from Failure — розділ SRE Workbook із поганим і добрим постмортемом того самого інциденту та поясненням, чому кожен із них саме такий.
- Example Postmortem — повний постмортем вигаданого збою з подальшими діями, висновками й хронологією.
- Managing Incidents — розділ 14 книги SRE: керівник інциденту, живий документ інциденту і передавання справ, на які згодом спирається постмортем.

Словник

Обирайте за фактичними умовами

Опишіть шлях розгортання, експлуатаційні ризики та чергову команду. Ми можемо визначити зміну з перевірками, шляхом відновлення та чіткою відповідальністю.

Дивитися, скільки це коштує Зв'язатися з нами →

Зробіть термінологію практичною

Запитайте, як «Що таке постмортем?» стосується вашої організації. Конкретного прикладу з поточної системи достатньо для початку розмови.

Переглянути наші послуги

welcome@engineer.company +45 50 10 61 84 Копенгаген, Данія

Візьміть цю сторінку із собою

Візитівка

Дбайливо зроблено з любов'ю — D.

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

Авторське право © 2025 – дотепер · Engineer ApS · Усі права захищено.

Надруковано з https://engineer.company/uk/glossary/postmortem/