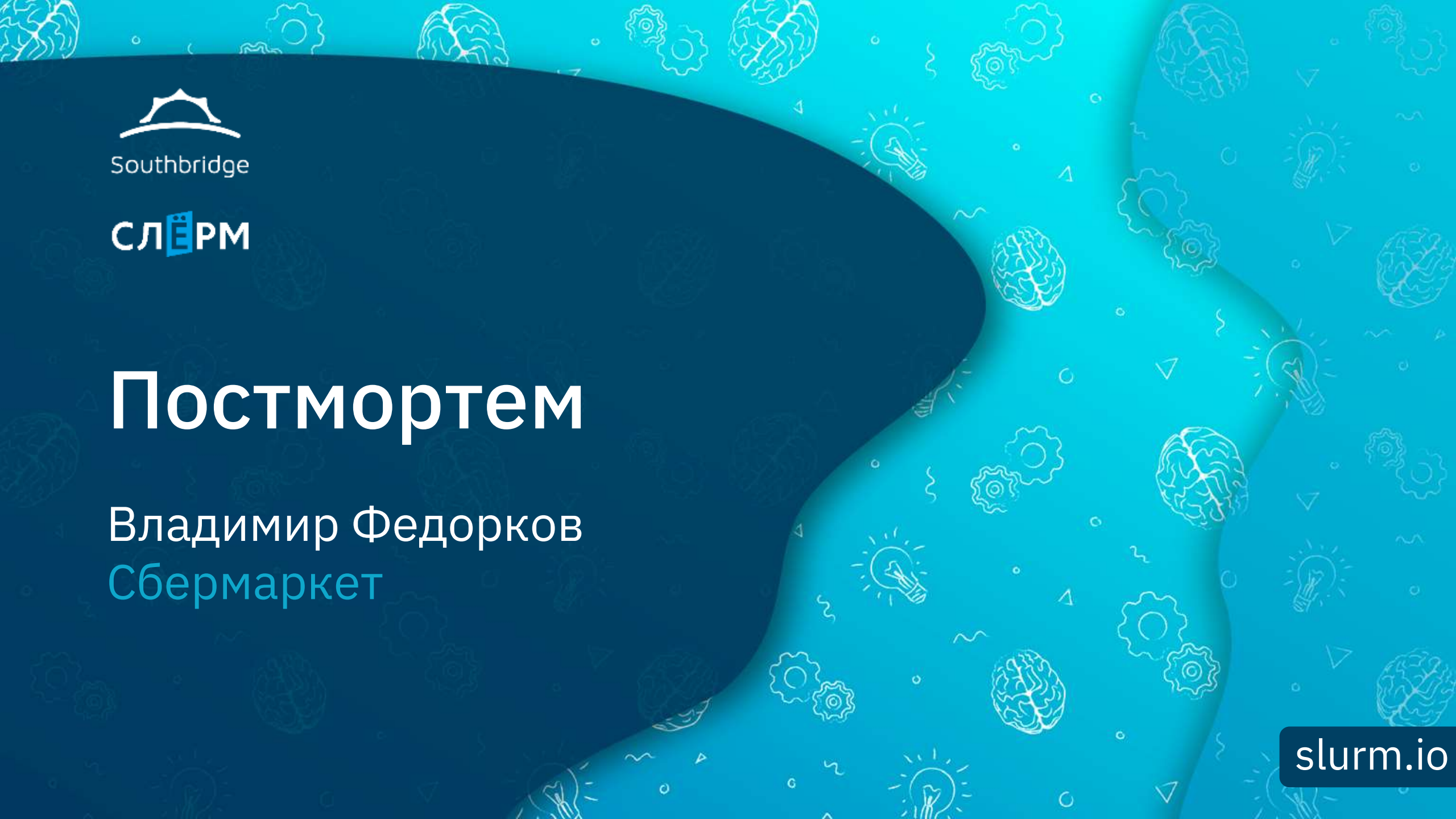


Постмортем

Владимир Федорков
Сбермаркет

slurm.io

Прод – это весело!

- То, что сделано – рано или поздно ломается
- Причем не «если», а «когда»
- Когда ломается первый раз – это бывает
- Если ломается второй – напрягает
- Если в третий
- … да еще в том же самом месте …
- … да еще за неделю….

СЛЁРМ

Чем отличается алерт от инцидента?

- Алерт это внутреннее событие эксплуатации
- Инцидент – событие компании
- Если алерт сопровождается потерями компании – это уже инцидент
- НО!
- Быстро поднятое упавшим не считается!
- Влияние должно быть существенным.
- Порог регламентируется политикой инцидент менеджмента

СЛЁРМ

PostMortem

An autopsy (a **post-mortem** examination)
is a surgical **procedure** that consists of a
thorough **examination of a corpse** by dissection
to determine the **cause**,
mode,
and **manner** of death
or to **evaluate** any disease
or **injury** that may be present
for **research** or **educational** purposes

СЛЁРМ

PostMortem это учёба на ошибках

Анализируем произошедшее, но смотрим только вперед

СЛЁРМ

Цель для бизнеса

- Убедиться, что больше такого не повторится
- Внести высокоуровневые изменения (если совсем все плохо)
- Если нужно, выделить необходимые ресурсы
- Право и обязанность инженеров эти ресурсы потребовать

СЛЁРМ

Цель инженеров

- Осознать, что нужно было сделать по-другому
- И как
- Что в поменять системе
- Какие перестроить процессы

СЛЁРМ

Постмортем без инцидента – деньги на ветер

- Инцидент (тикет) заводится специально обученным человеком
- Его называют «Дежурный инженер», «Инцидент менеджер» или «SRE»
- Еще в процессе работы над инцидентом
- В режиме стенограммы, но со точным (до минуты) временем
- Кто когда что наблюдал и что при этом делал
- Чем все закончилось
- Какие костыли остались в системе после инцидента

СЛЁРМ

Что нужно для пост-мортема

- Инцидент
- Ключевые участники
- Таймлайн
- Детальное описание произошедшего
- Рассчитанное влияние
- Свежие воспоминания
- Время на post-mortem от 30 минут до 2 часов

СЛЁРМ

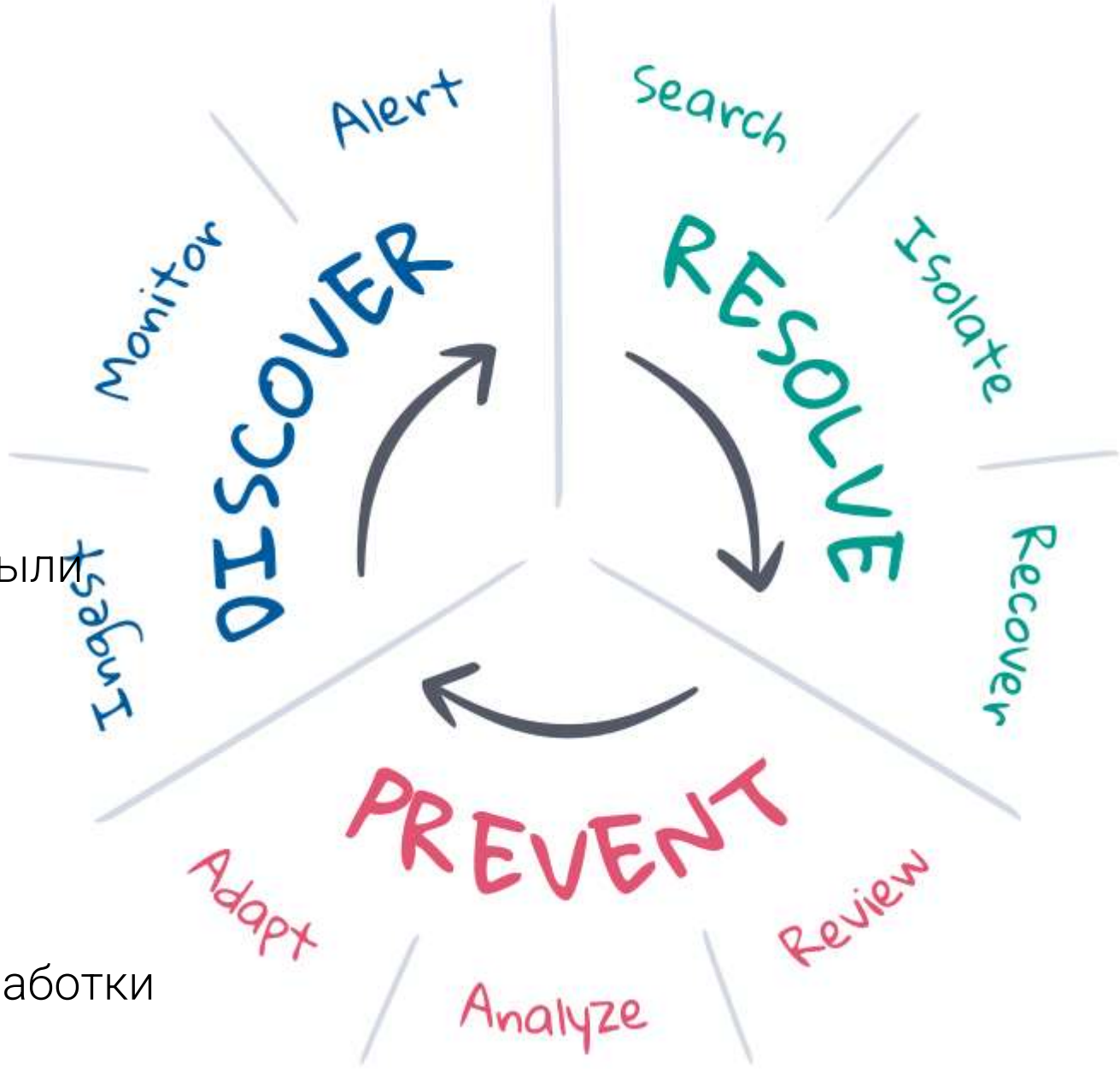
Blameless culture

- Мы не показываем пальцем на того, кто ошибся
- И никого не наказываем
- По крайней мере первые десять раз!!!
- Иначе мы не получим нужной прозрачности
- Нет прозрачности – нет культуры, есть политика
- Есть политика – нет инженеров, есть политики
- Это не то место, где можно учиться

СЛЁРМ

Вопросы PostMortem

- Что пошло не так
- Что сработало как надо
- Чем заменяем поставленные костыли
- - В инфраструктуре
- - В коде
- - В процессах
- Какие нужны долговременные наработки



СЛЁРМ

Откуда взялись костыли?

- Нужно минимизировать аффект на пользователя
- Срочным, быстрым фиксом
- Как можно быстрее
- Потому что не до «чистых» методов
- Прод горит
- Это только первый шаг
- Следующий шаг – замена фикса на решение

СЛЁРМ

Результаты PostMortem

- Список разумных задач решающих инцидент
- Инцидент не решен, пока задачи не выполнены
- Для каждой задачи есть ответственный
- Есть сроки
- Потому что пока нет фикса ситуация может повториться
- В идеале фикс тестируется на схожей ситуации
- Есть куча других граблей, которые нас очень ждут!
- От теории к практике!

СЛЁРМ

Шаблон PostMortem

Факты

- Название инцидента
- Приоритет
- Как узнали
- Влияние
- Таймлайн инцидента
  - Кто участвовал
  - Что делали

Рефлексия

- Суть инцидента
- Root cause
- Что пошло не так
- Что отработало как нужно
- Action items
- Lessons learned

СЛЁРМ

Приоритет

- P0 / Security – Высший приоритет
- P1 / Critical – Отказ основной функциональности дольше 5 минут
  и/или потери компании больше 1 000 000 рублей
- P2 / Major – Деградация основной функциональности
  и/или потери больше 200 000 рублей
- P3 / Normal – отказ или деградация сервисной функциональности с риском потери

СЛЁРМ

Кто сообщил?

- Отвечаем на вопрос: по какому каналу пришла информация об инциденте?
- Можно ли было узнать быстрее?
- Достаточно ли хорошо работает наш мониторинг?
- Какие были предпосылки для инцидента?
- Можно ли их было заметить и предотвратить инцидент?

Влияние

- На работу каких компонентов повлиял инцидент (SRE, DevOPs)
- Какой был аффект на пользователей (SRE)
- Сколько по времени было влияние (SRE, DevOps)
- Сколько прямых убытков понесла компания (SRE, Бизнес)
- Оценка долговременных потерь от инцидента (Риск-менеджеры)

СЛЁРМ

Timeline

- Когда и кто заметил
- Куда смотрели, что видели
- Как происходила эскалация
- Была ли эскалация успешной
- Какие гипотезы выдвигали
- Кто и что делал для проверки
- Как менялось влияние
- Что привело к восстановлению функциональности

СЛЁРМ

Root cause / Первопричина

- Какое событие изначально привело к развитию инцидента?
- В чем его причина?
- Как его можно избежать

СЛЁРМ

Что пошло не так?

Какие процессы дали сбой?

- Где стормозили
- Чего не заметили
- Что упустили
- Где ошиблись
- Что сделать не успели
- Где не хватило знаний и опыта

СЛЁРМ

Что отработало как нужно

Отмечаем людей и процессы

- Какие процессы отработали как надо
- Какая информация о системе помогла? Графики, логи, etc
- Что помогло найти причину
- Что хорошего мы можем отметить в коммуникации
- Какие люди помогли починить прод

Action items

Разгребаем последствия инцидента

- Какие костыли нужно убрать из системы?
- Какие доработки мы должны сделать, что бы в такой же ситуации инцидент не повторился?
- Как мы можем улучшить тестирование, что бы ловить похожие проблемы?
- Какие процессы нужно поменять и как?

СЛЁРМ

Lessons learned

Рефлексия по инциденту в целом

- Можно ли было избежать инцидента?
- Можно ли было уменьшить или совсем избежать влияния?
- Что нужно поменять прямо сейчас?
- В каких командах есть пространство для улучшений?

СЛЁРМ

Раз в неделю – ретро по инцидентам

Рефлексия по общей стабильности

- Какие инциденты происходили?
- В какую сторону движется наша стабильность?
- Что мы делаем прямо сейчас, что бы улучшить стабильность?
- Что еще нужно сделать?
- Какие глобальные стратегии нужно поменять и как что бы наша долговременная стабильность увеличилась?

СЛЁРМ

Так зачем эти все постмортемы?

- Инцидент это реактивная работа
- Очень дорого
- Попытка перевести работу в проактивную
- Хотя бы часть
- Не прыгать на одни и те же грабли два раза
- Это просто стыдно

СЛЁРМ

Как мы работаем с постмортемами

- Выбираем любой кейс
- Берем шаблон https://docs.google.com/document/d/1DahPwEq_JTtG-v32GHBI8E-dYFmZ0G9YYxKJL_rqABI
- Заполняем постмортем
- Тегаем спикера в чате

СЛЁРМ

PostMortem

Вопросы-предложения-замечания

СЛЁРМ

PostMortem

Пока не попробуете – не научитесь.

Лучше читать чужие postmortem

Только не на ночь!

СЛЁРМ