Security team

Agile и SOC
Миф или реальность?

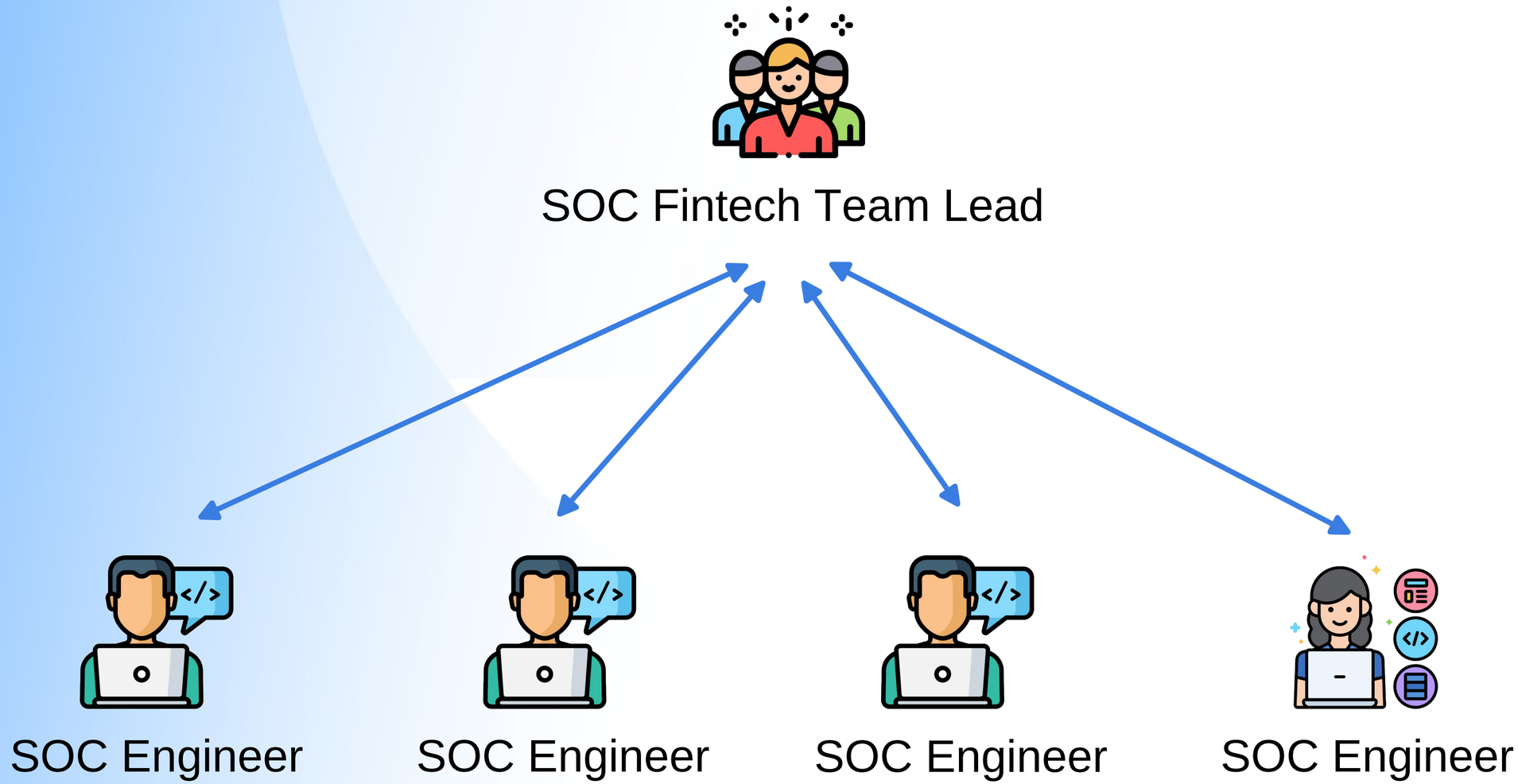
07.12.23

Никита Курганов

whoami

- 26 лет
- Senior Fintech SOC Engineer
- Окончил ИУ-8 & Аспирант МГТУ им. Н.Э.Баумана
- 2 года в Kaspersky – Junior Malware Analyst
- 2 года в Сбербанке – Lead Security Expert
- 1 патент и 3 выступления на крупных ИБ конфах + выступление на SAS

Действующие лица



Действующие лица

SOC Fintech Team Lead

?

SOC Engineer

SOC Engineer

SOC Engineer

SOC Engineer

Решаемые задачи

Дежурство

- Разбор алертов на линиях SOC
- Починка логов

Решаемые задачи

Дежурство

- Разбор алертов на линиях SOC
- Починка логов

Проектные задачи

- Разработка алертов
- Подключение логов
- Администрирование и улучшение SIEM
- Пилотирование продуктов
- Аудиты (PCI DSS, ГОСТ 57580)

Решаемые задачи

Дежурство

- Разбор алертов на линиях SOC
- Починка логов

Проектные задачи

- Разработка алертов
- Подключение логов
- Администрирование и улучшение SIEM
- Пилотирование продуктов
- Аудиты (PCI DSS, ГОСТ 57580)

Инциденты

Участие в инцидентах ИБ и их разбор

Sprint 2 недели

Security team

Инструменты

1:1 sync

В начале неделе личное общение с каждым инженером в команде

Инструменты

Grooming

Приоритизируем задачи от смежных команд

1:1 sync

В начале неделе личное общение с каждым инженером в команде

Инструменты

Grooming

Приоритизируем задачи от смежных команд

1:1 sync

В начале неделе личное общение с каждым инженером в команде

Летучка SOC Fintech

Инструменты

Grooming

Приоритизируем задачи от смежных команд

Poker/Retro

Подводим итоги недели, выставляем трудозатраты задачи

1:1 sync

В начале неделе личное общение с каждым инженером в команде

Летучка SOC Fintech

Инструменты

Grooming

Приоритизируем задачи от смежных команд

Poker/Retro

Подводим итоги недели, выставляем трудозатраты задачи

Story points

1:1 sync

В начале неделе личное общение с каждым инженером в команде

Летучка SOC Fintech

Инструменты

Grooming

Приоритизируем задачи от смежных команд

Poker/Retro

Подводим итоги недели, выставляем трудозатраты задачи

Story points

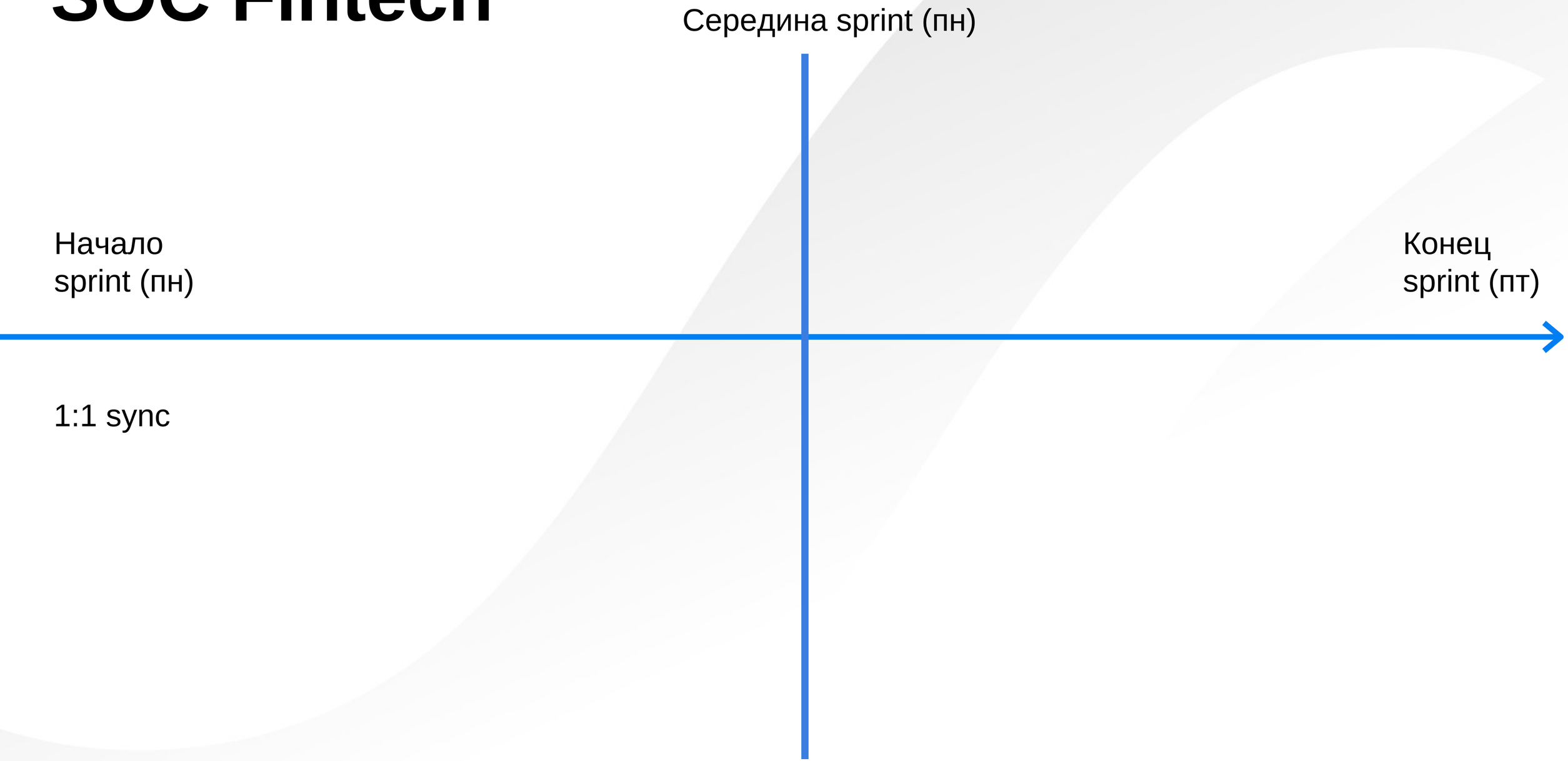
1:1 sync

В начале неделе личное общение с каждым инженером в команде

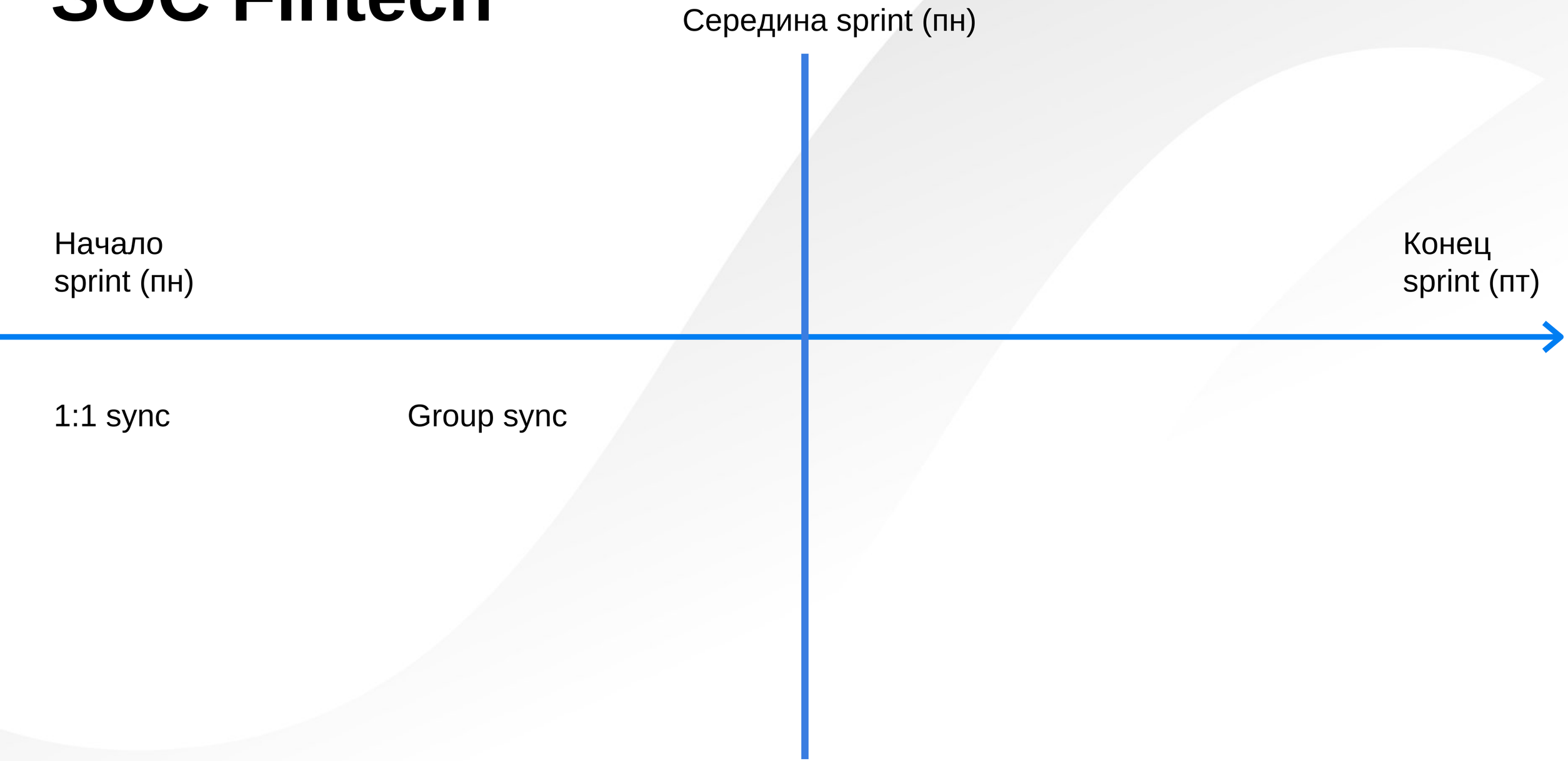
Летучка SOC Fintech

Доска задач/тикет система

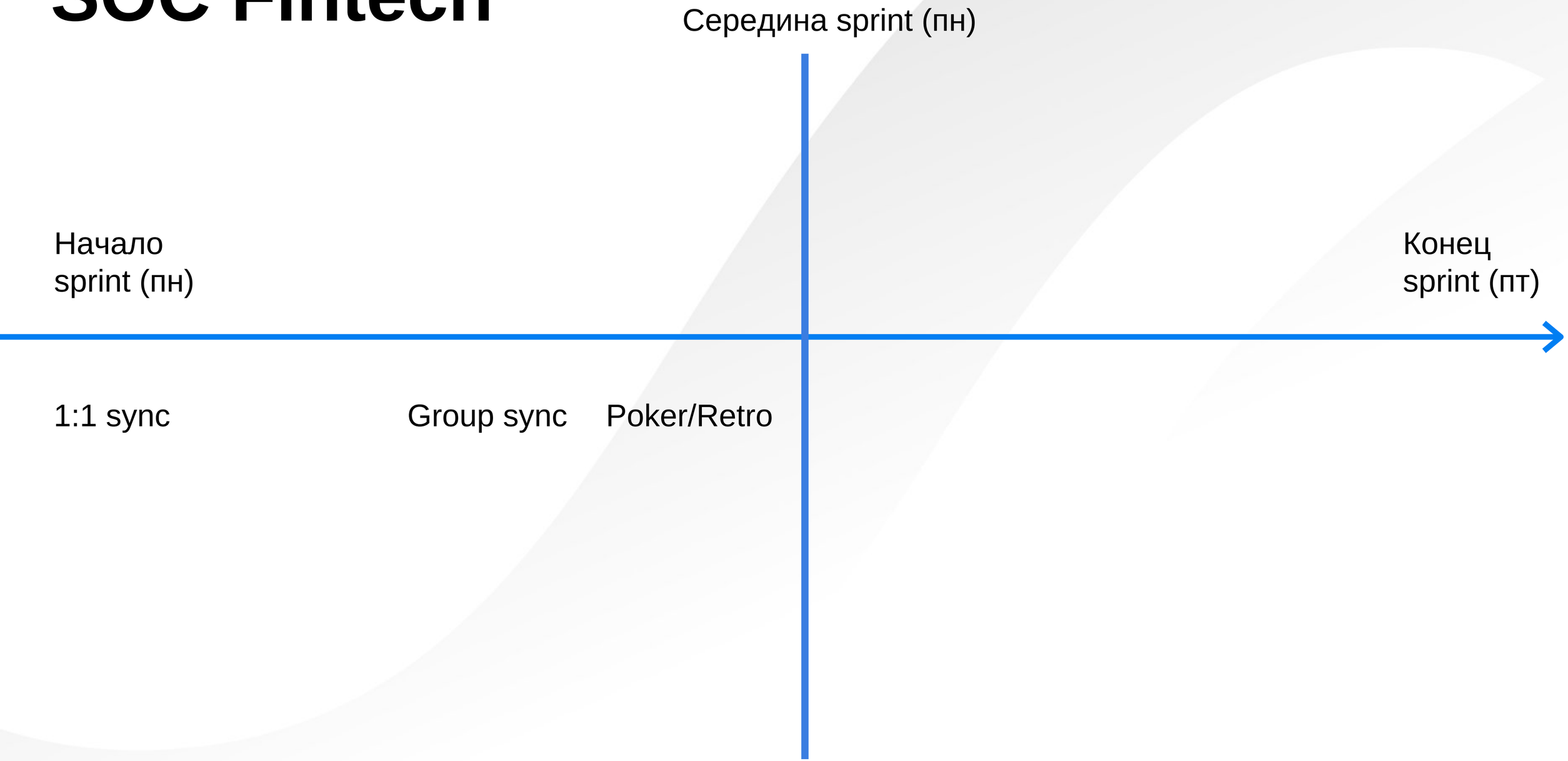
SOC Fintech



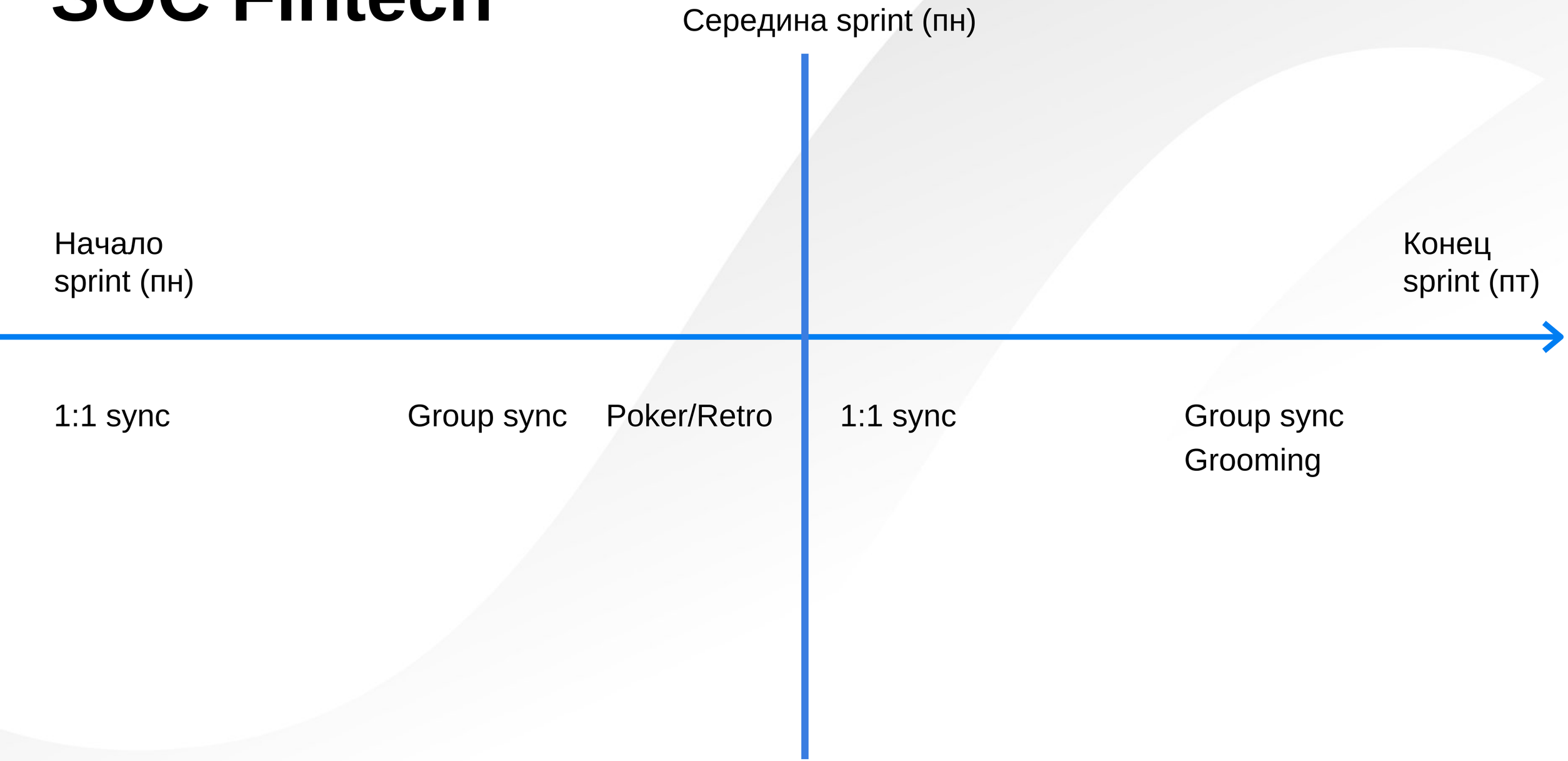
SOC Fintech


Середина sprint (пн)
Начало
sprint (пн)
Конец
sprint (пт)
1:1 sync
Group sync

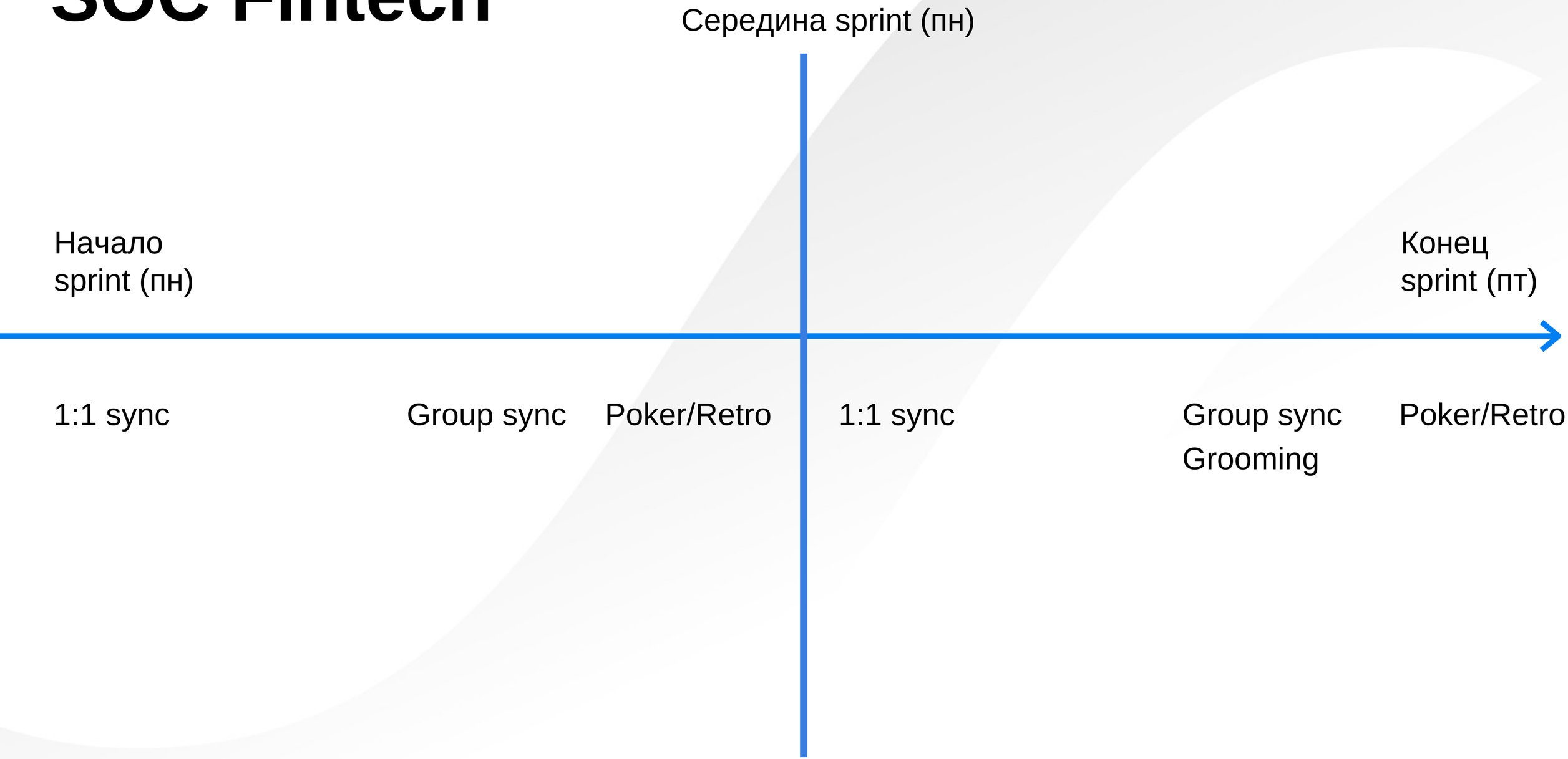
SOC Fintech


Середина sprint (пн)
Начало
sprint (пн)
Конец
sprint (пт)
1:1 sync
Group sync
Poker/Retro

SOC Fintech


Середина sprint (пн)
Начало
sprint (пн)
Конец
sprint (пт)
1:1 sync
Group sync
Poker/Retro
1:1 sync
Group sync
Grooming

SOC Fintech


Середина sprint (пн)
Начало
sprint (пн)
Конец
sprint (пт)
1:1 sync
Group sync
Poker/Retro
1:1 sync
Group sync
Grooming
Poker/Retro

1 SP = 2ч рабочего времени

Правила

1

- 80% времени от спринта на задачи
- 20% времени на инциденты и внеплановые задачи

Правила

1

- 80% времени от спринта на задачи
- 20% времени на инциденты и внеплановые задачи

2

На спринт не более 3-4 задач (суммарно не более 40 SP) !!!

Правила

1

- 80% времени от спринта на задачи
- 20% времени на инциденты и внеплановые задачи

2

На спринт не более 3-4 задач (суммарно не более 40 SP) !!!

3

Эпики (большие задачи) разделяй на мелкие задачи

Правила

1

- 80% времени от спринта на задачи
- 20% времени на инциденты и внеплановые задачи

2

На спринт не более 3-4 задач (суммарно не более 40 SP) !!!

3

Эпики (большие задачи) разделяй на мелкие задачи

4

Разделяй и властвуй

- Свои задачи и задачи от смежников
- Алерты и проектные задачи

Security team

Спасибо за внимание!

07.12.23

Никита Курганов