Product Security Topologies: применяем фреймворк Team Topologies, чтобы забустить безопасность

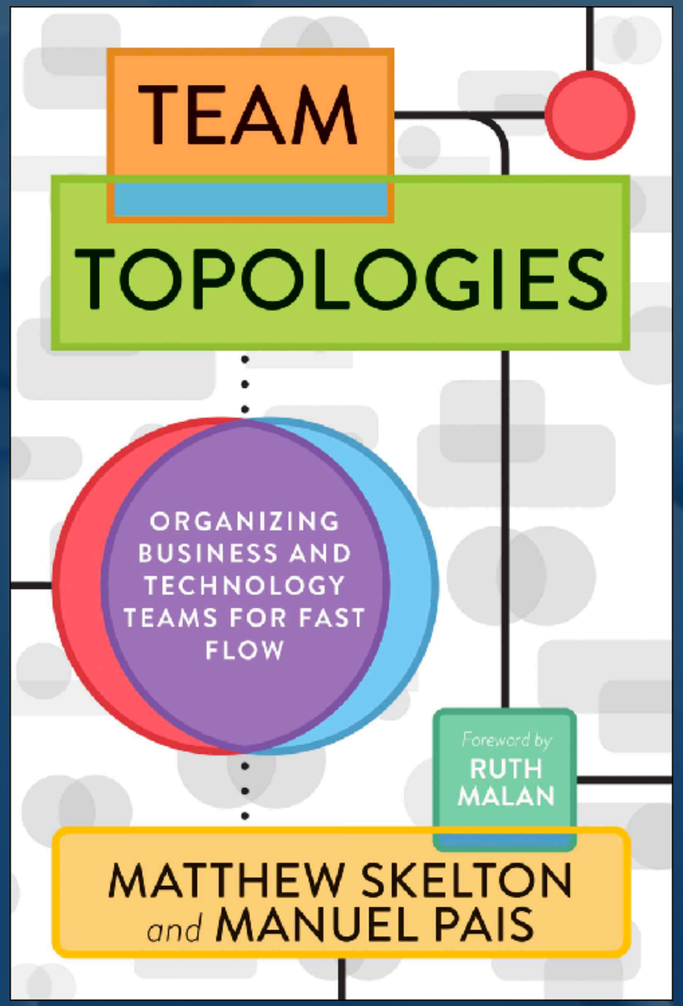
Вацлав Довнар

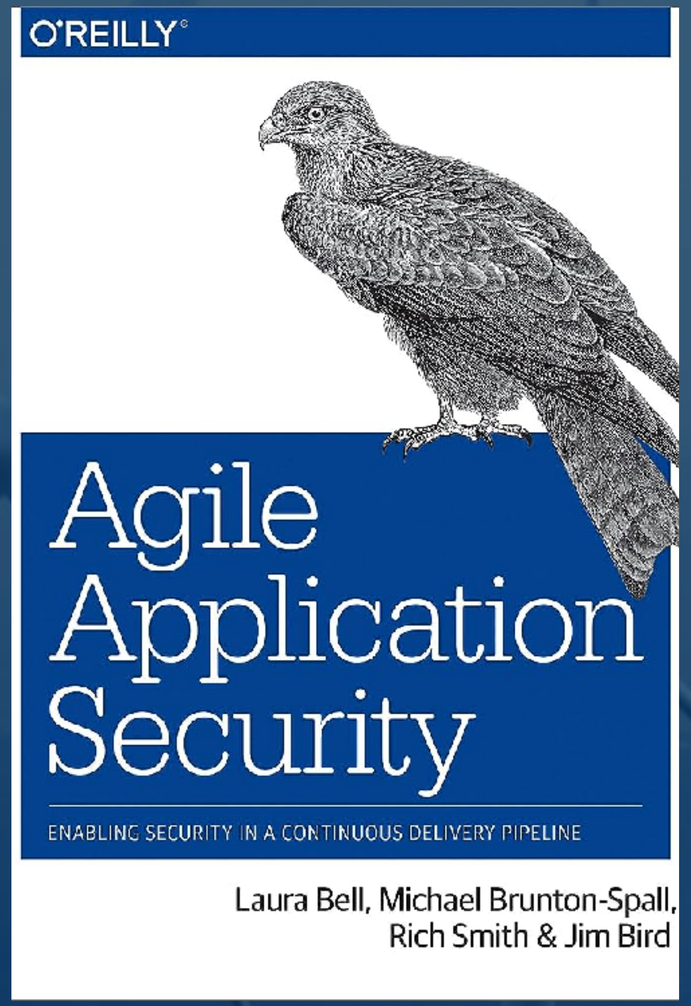
Profile

Вацлав Довнар

Независимый исследователь

Опыт: 10 лет в ИБ


TEAM
TOPOLOGIES
ORGANIZING BUSINESS AND TECHNOLOGY TEAMS FOR FAST FLOW
Foreword by
RUTH MALAN
MATTHEW SKELTON
and MANUEL PAIS


O'REILLY
Agile Application Security
ENABLING SECURITY IN A CONTINUOUS DELIVERY PIPELINE
Laura Bell, Michael Brunton-Spall,
Rich Smith & Jim Bird

Какой концепт перешел из производства первых автомобилей в современное ИТ?

Team Topologies

- Подход Team First
- Прямой и обратный закон Конвея
- Team API
- 4 типа команд
- 3 типа взаимодействия

Team First

- Все необходимые ресурсы есть внутри команды
- Вся команда отвечает за итоговый результат

Team First и внешние зависимости

- Нельзя упаковать в команду все на всякий случай
- Рынок AppSec
- Время на онбординг

Team First & Security

Кто отвечает за безопасность продукта?

Руководство	➡️	принятие решение по риску / изменение приоритетов
ИБ	➡️	платформа, консалтинг, метрики, экспертиза
Команда продукта	➡️	ответственность за безопасность продукта

HighLoad++ 2022

[Продвинутые подходы построения AppSec]

Закон Конвея

- Организации обычно вынуждены создавать программное обеспечение, повторяющее систему реальных коммуникаций между сотрудниками

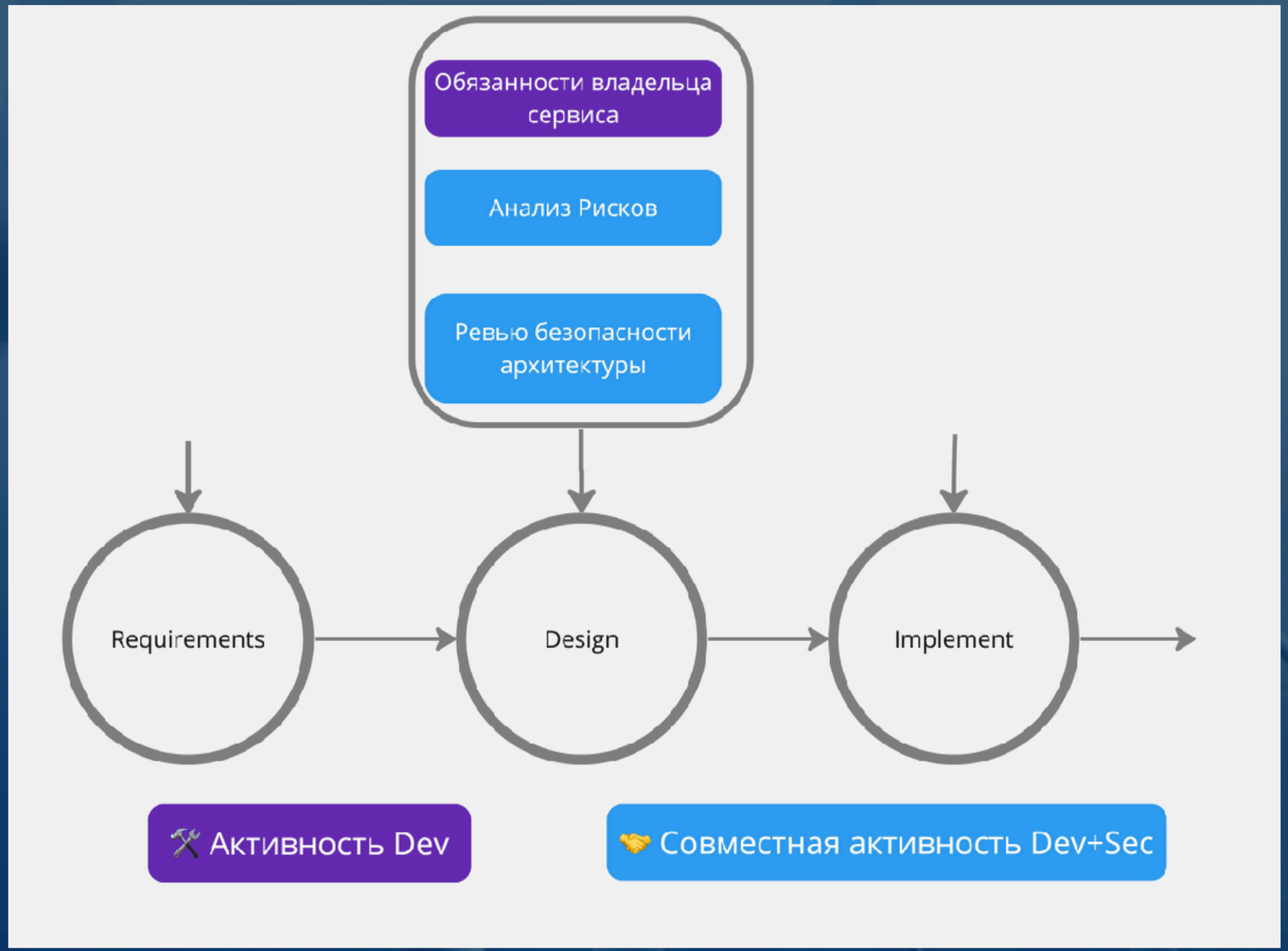
“If you have four groups working on a compiler, you’ll get a 4-pass compiler”

«Структура команды => архитектура системы => реализация системы»

Закон Конвея & Security

- Организации обычно вынуждены создавать ПО повторяющие системы связей в организации

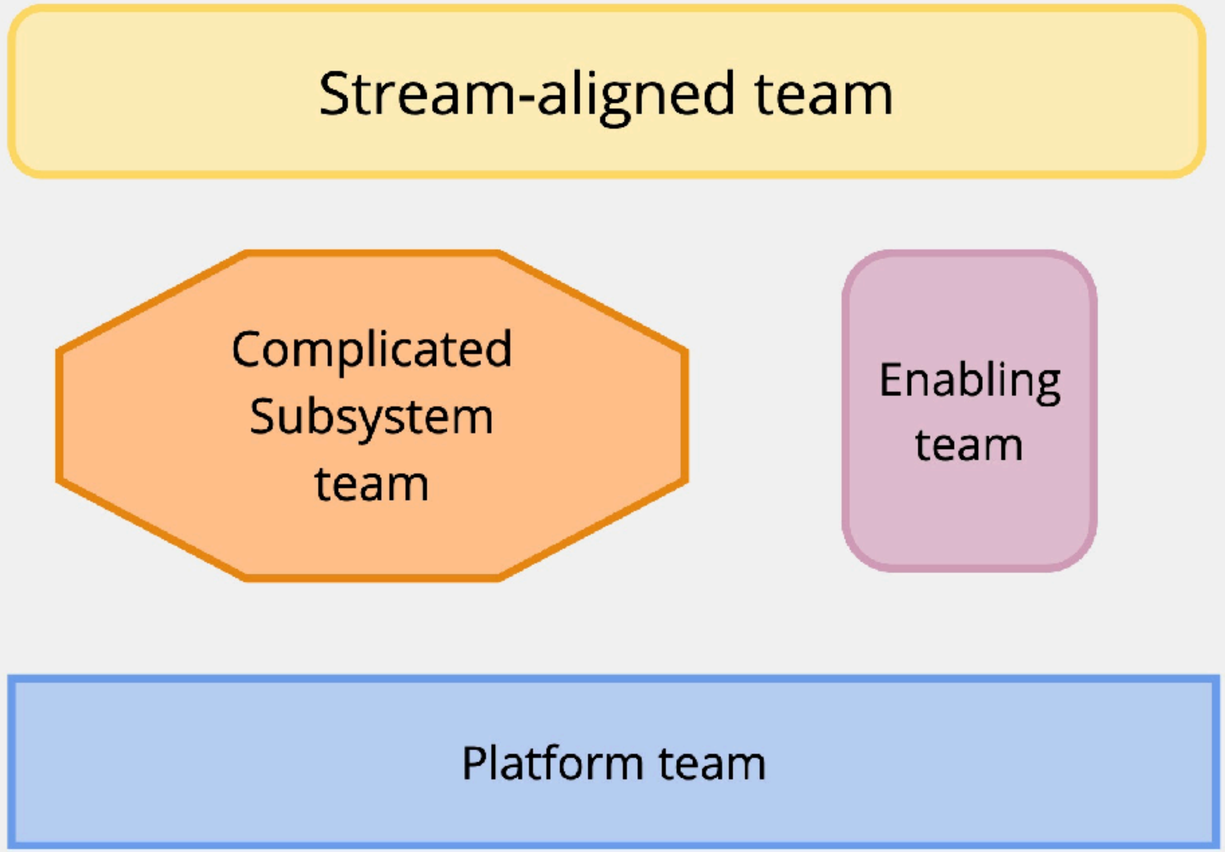
=> создавайте устойчивые коммуникации с привязкой к этапу разработки чтобы влиять на безопасность продукта


Обязанности владельца сервиса
Анализ Рисков
Ревью безопасности архитектуры
Requirements
Design
Implement
🛠️ Активность Dev
🤝 Совместная активность Dev+Sec

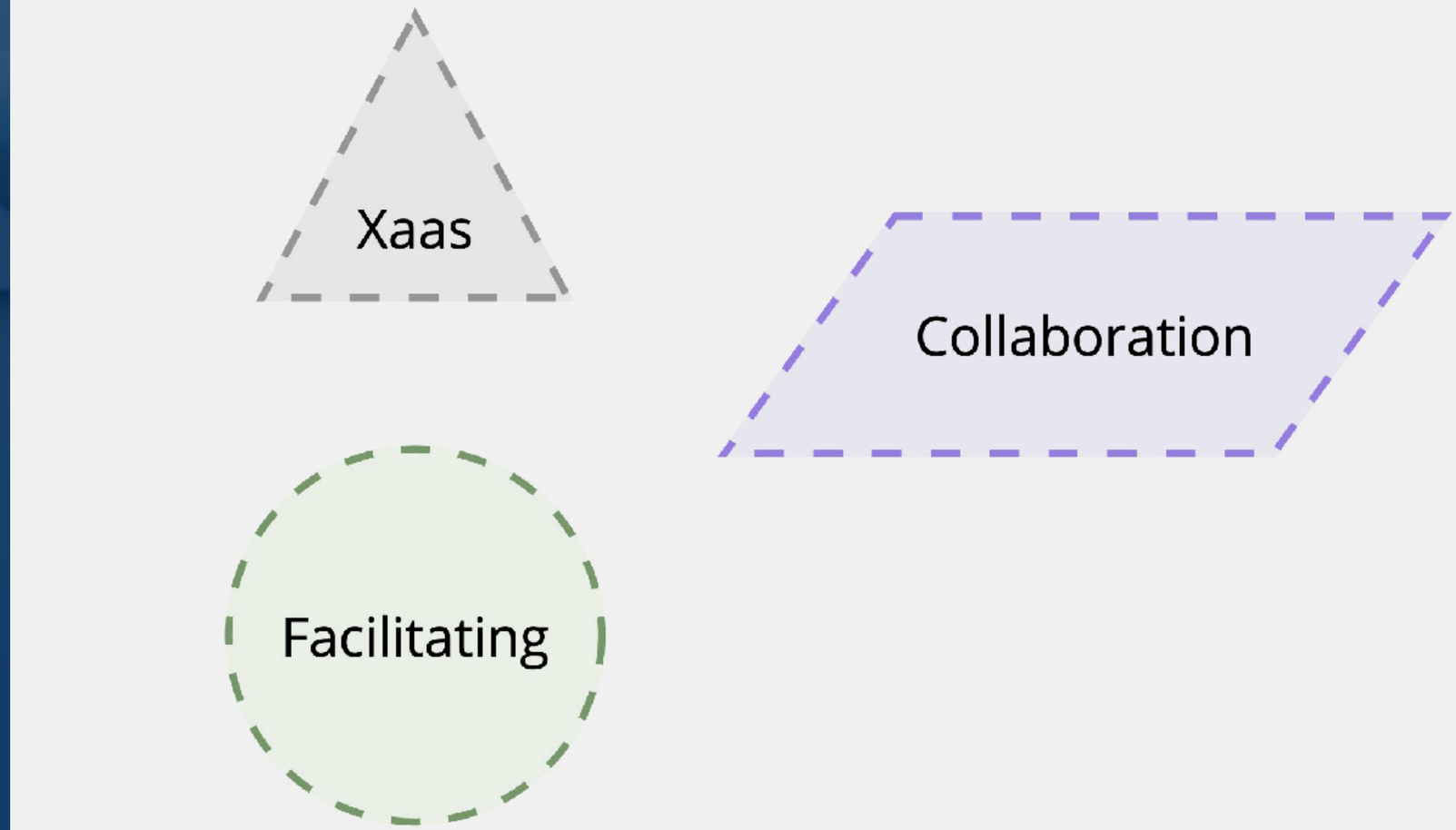
Team API

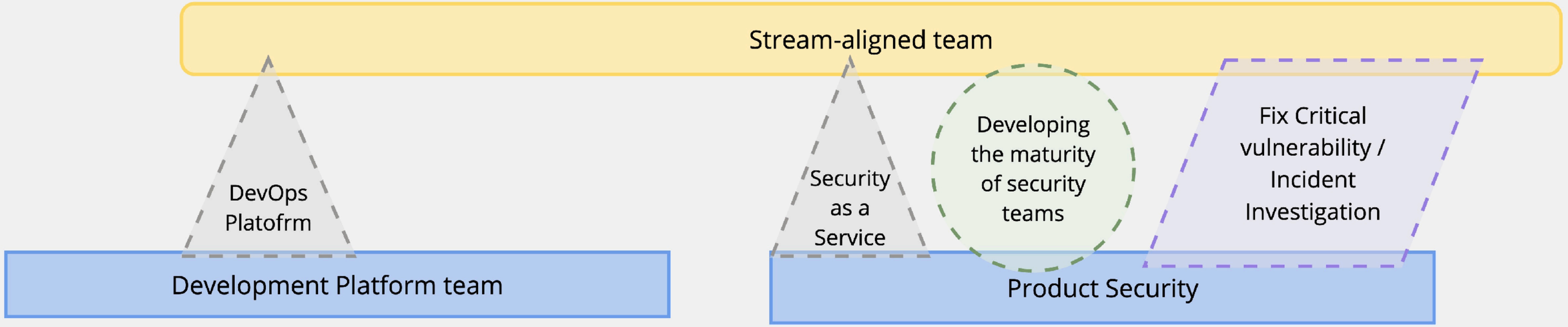
```
Team API
Team Name: Product Security
Team Type: Platform
Services:
  - Architecture Review
  - Threat Modeling
  - Security Audit
  - Investigation of incidents
Software owned:
  - GitLab
  - Nuclei
Wiki search terms:
  - security
  - appsec
Chat channels:
  - " product-security-team"
Time of daily sync meeting:
  - link to meeting
```

Типы команд

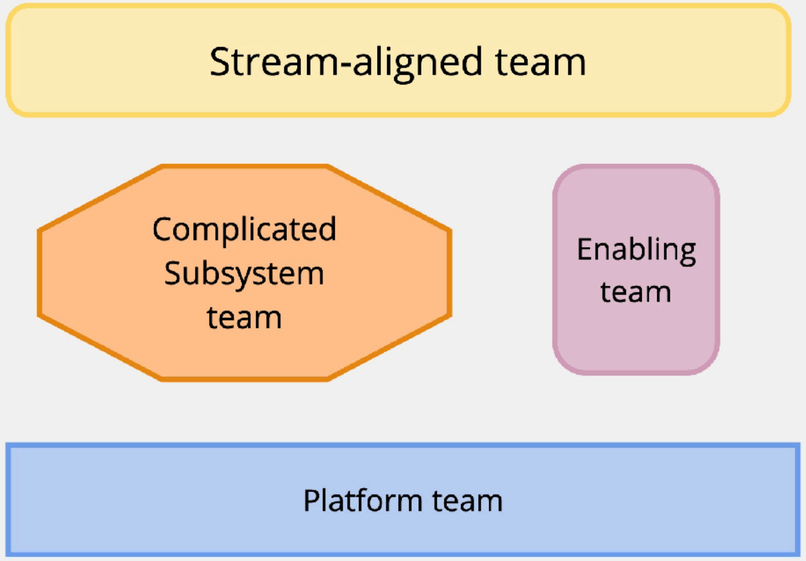

Stream-aligned team
Complicated Subsystem team
Enabling team
Platform team

Типы взаимодействия команд

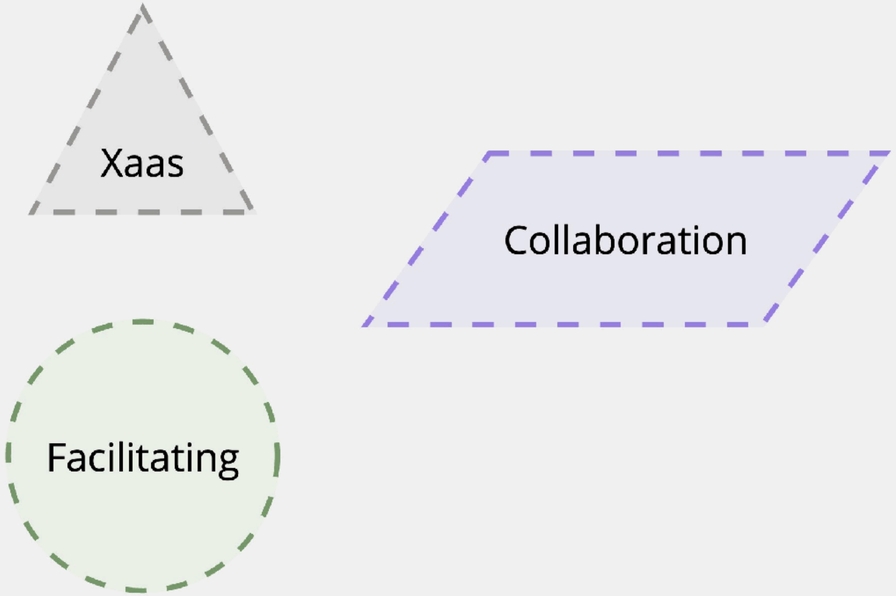


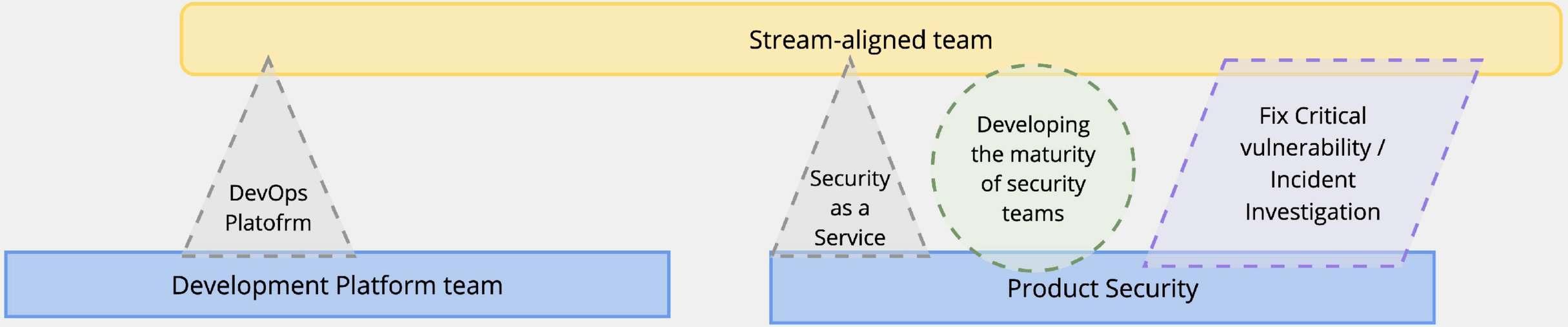


Типы команд

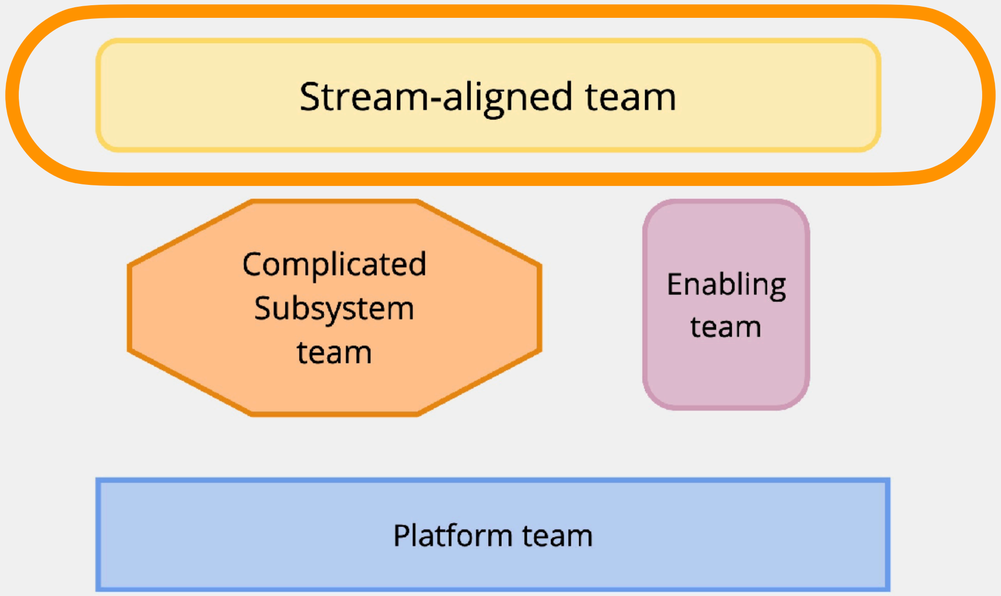


Типы взаимодействия команд

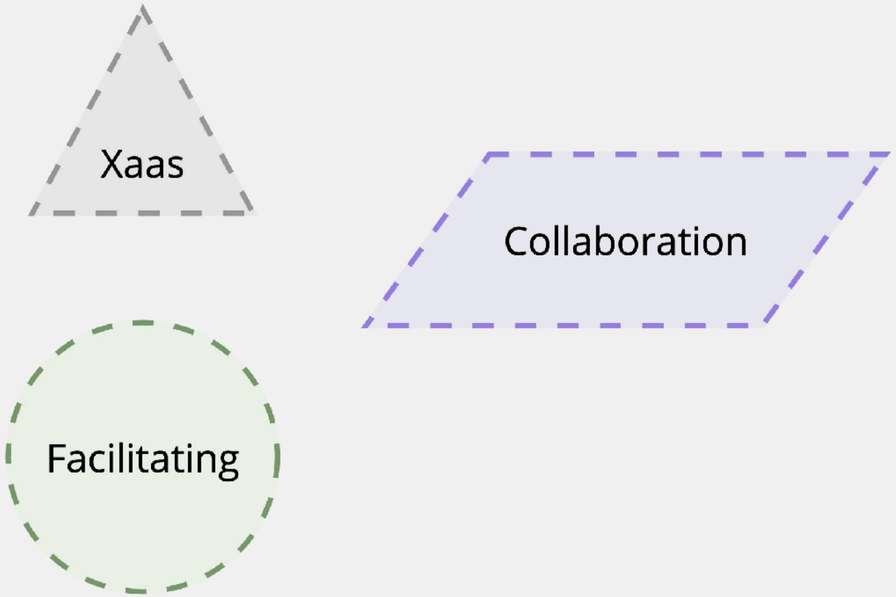


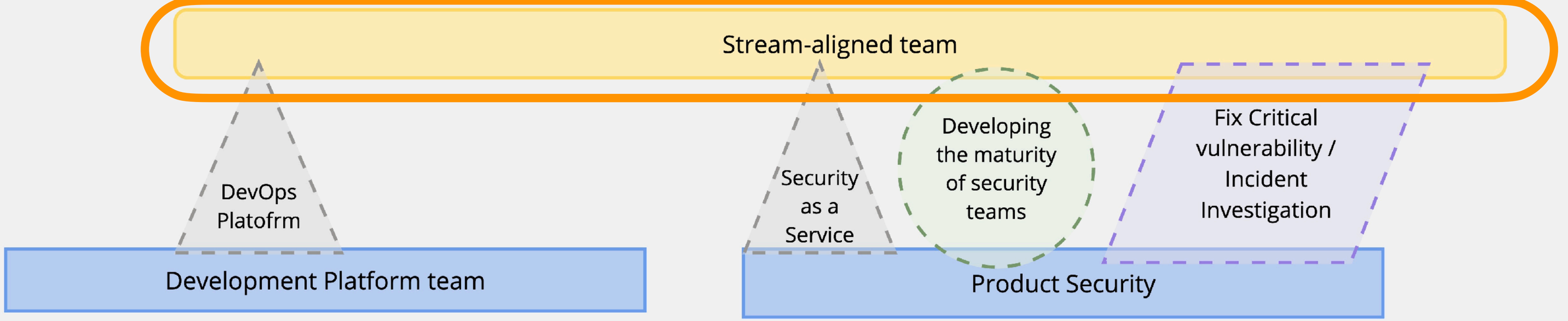


Типы команд

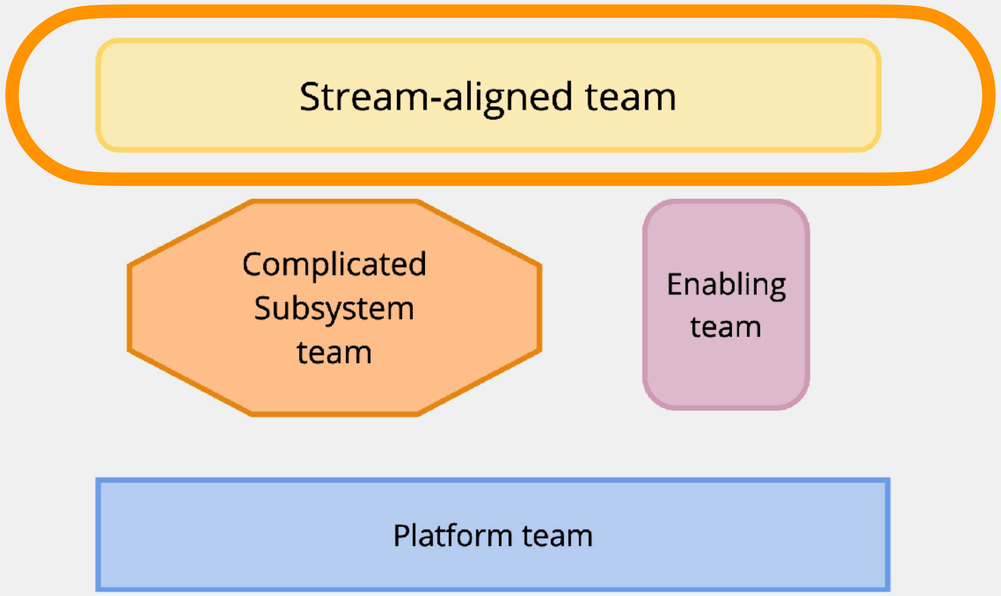


Типы взаимодействия команд

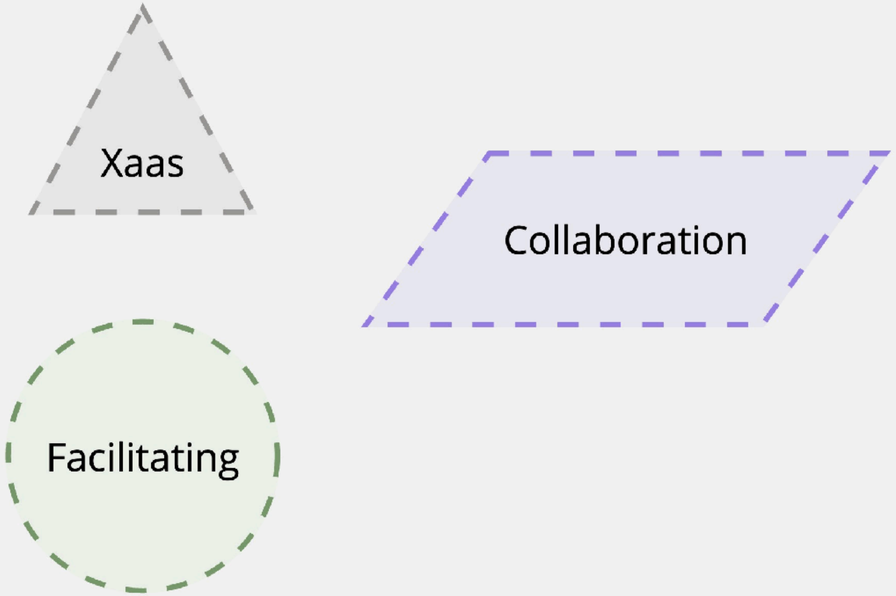


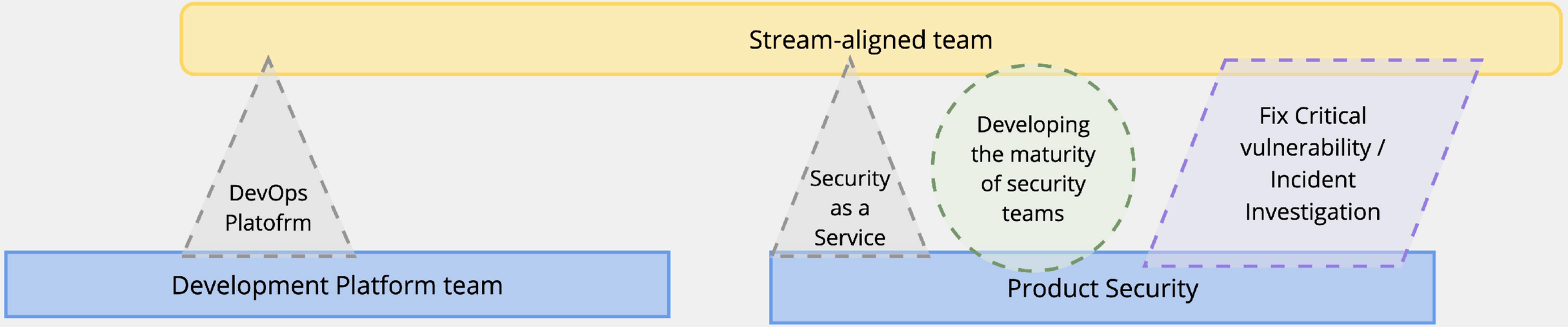


Типы команд

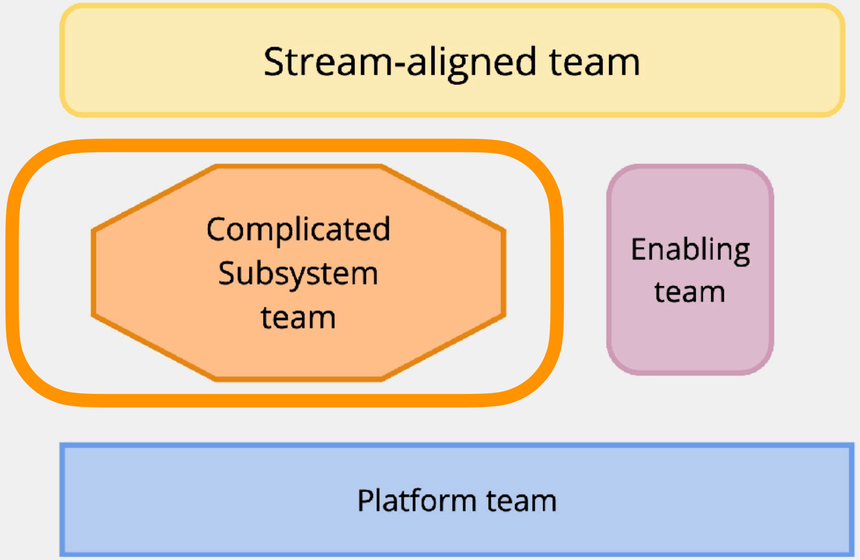


Типы взаимодействия команд

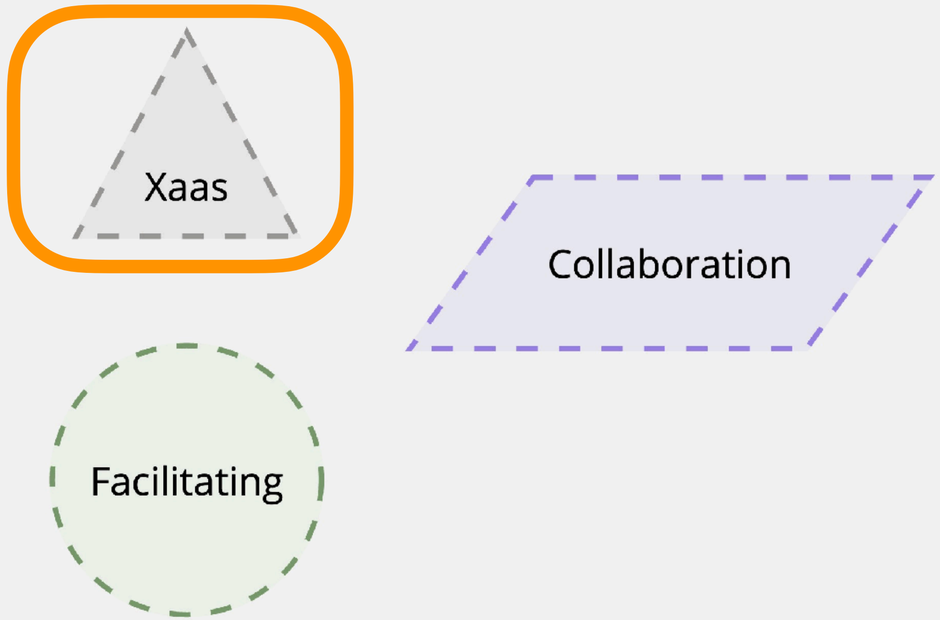


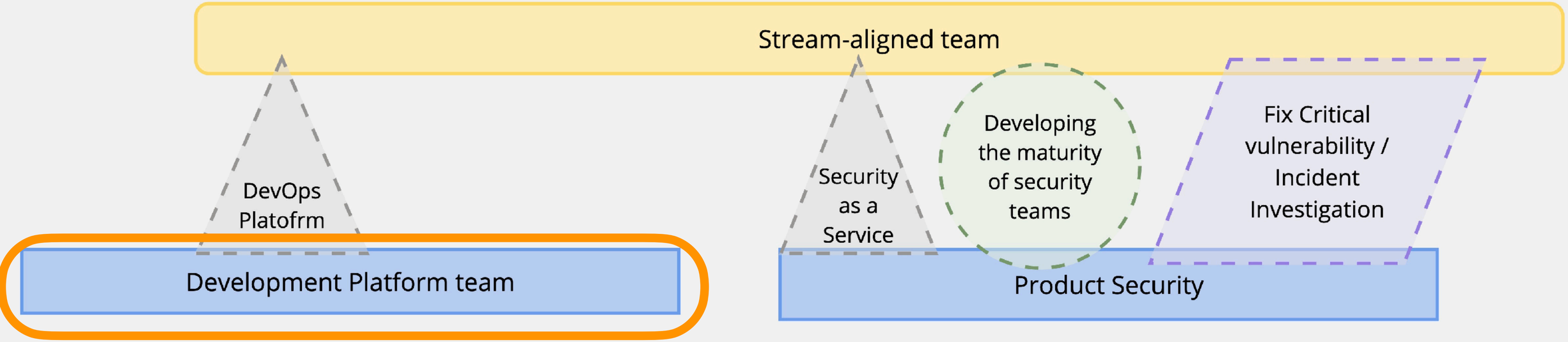


Типы команд

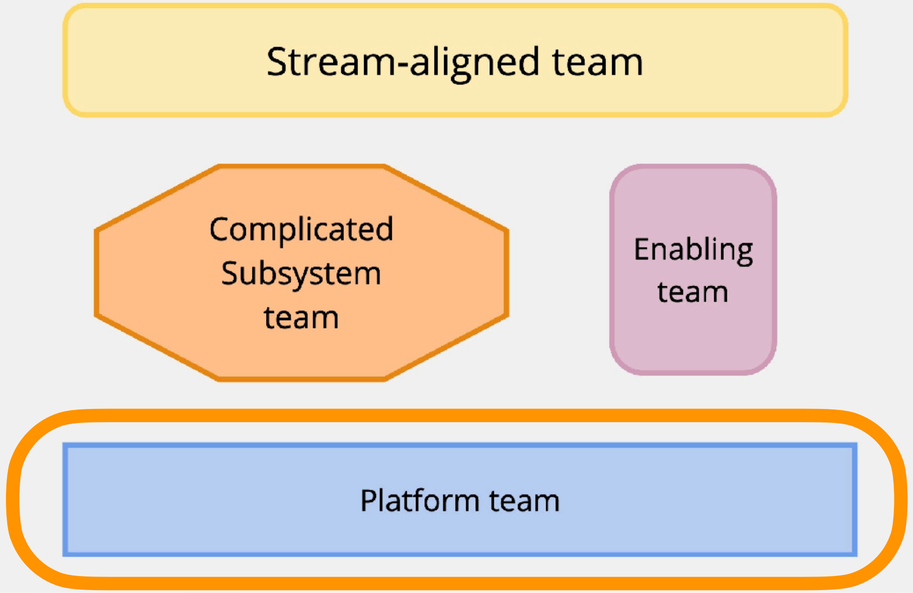


Типы взаимодействия команд

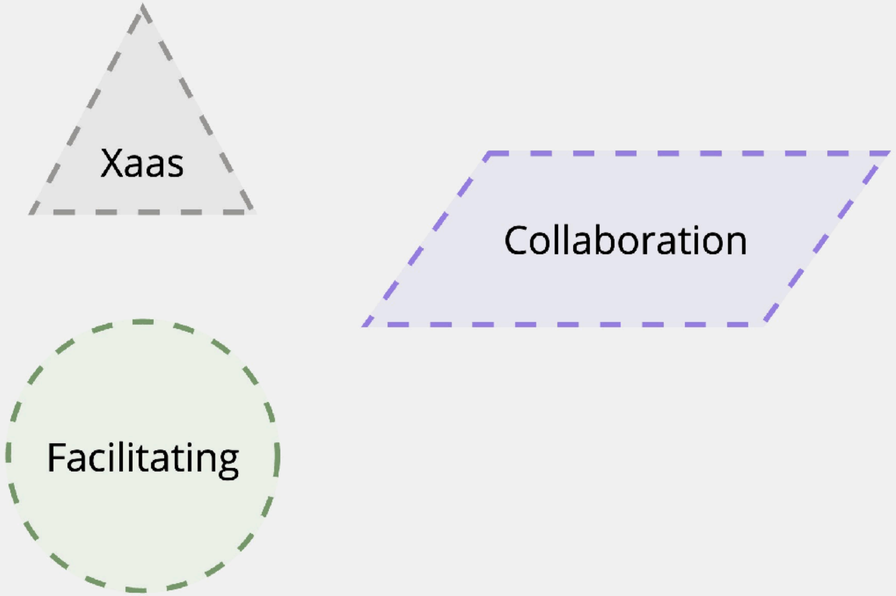


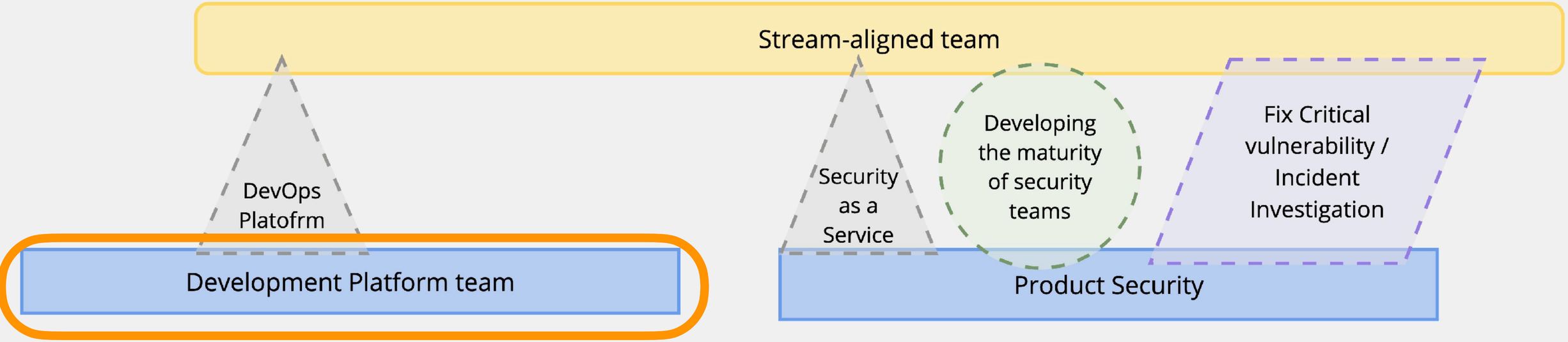


Типы команд

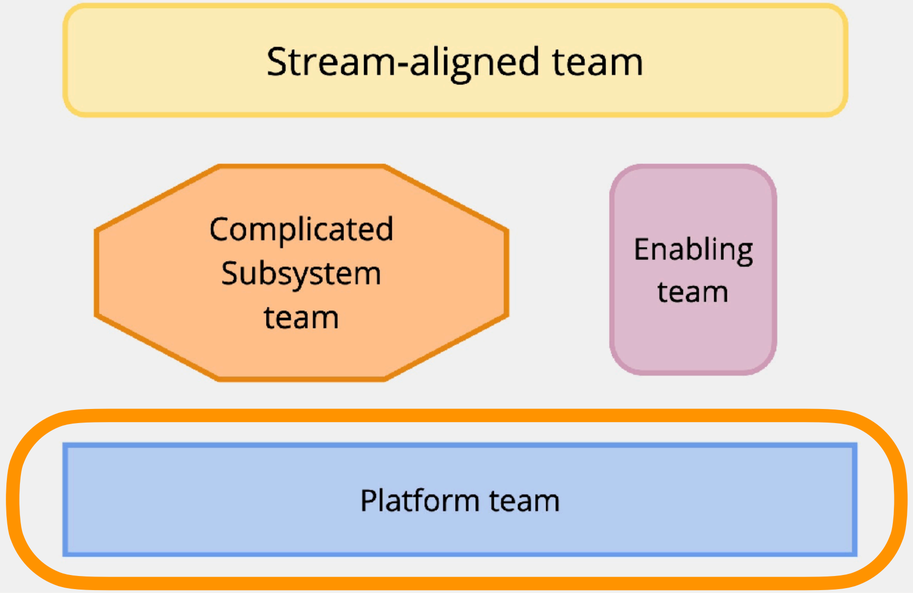


Типы взаимодействия команд

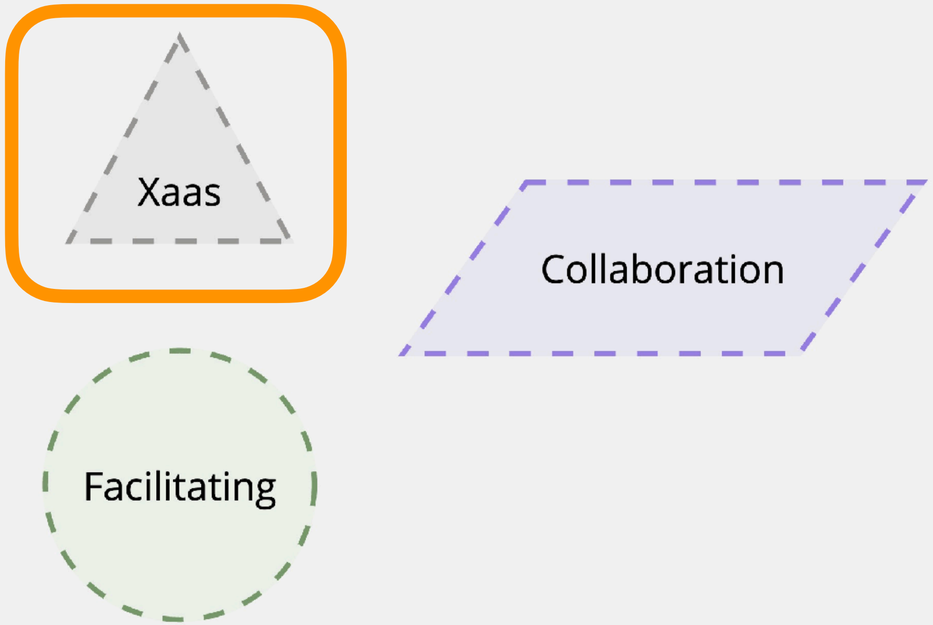


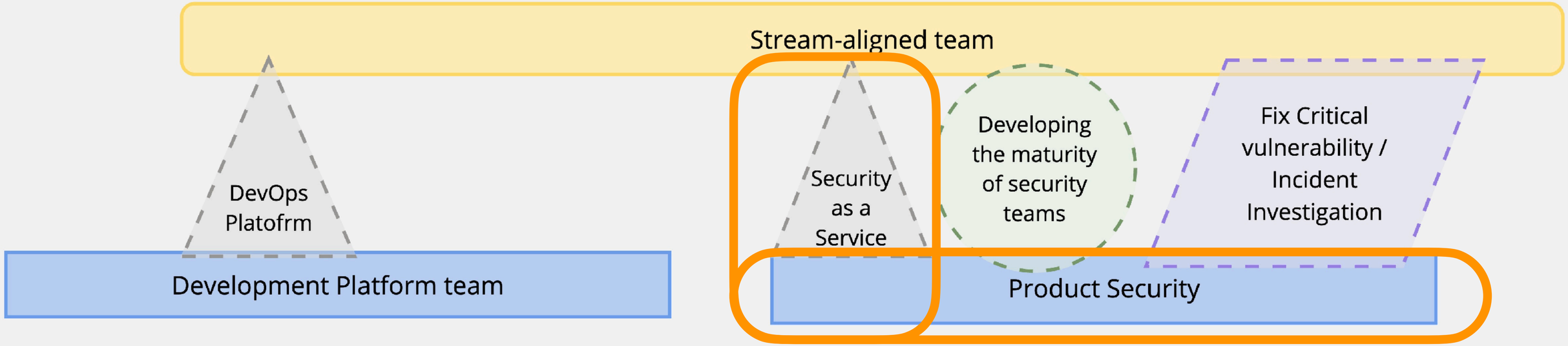


Типы команд

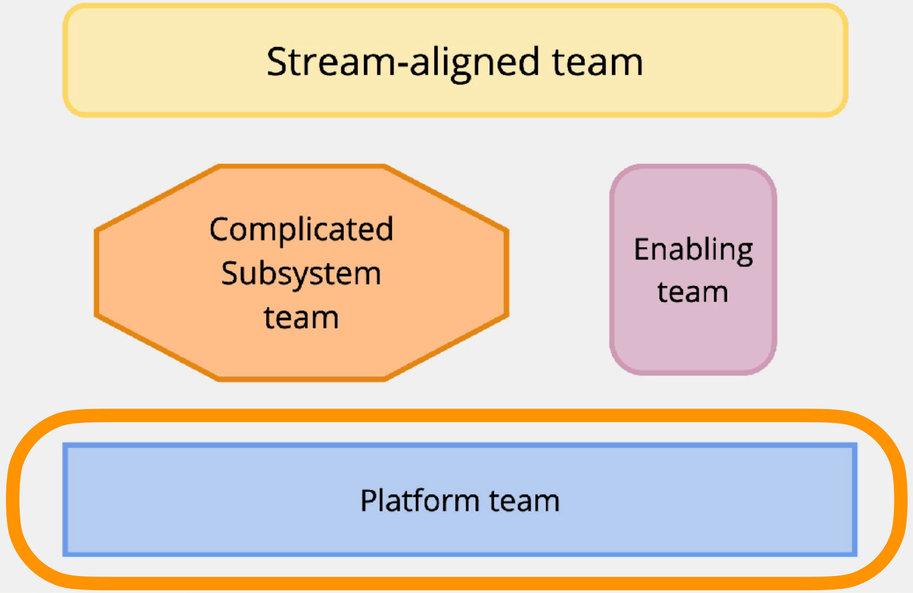


Типы взаимодействия команд

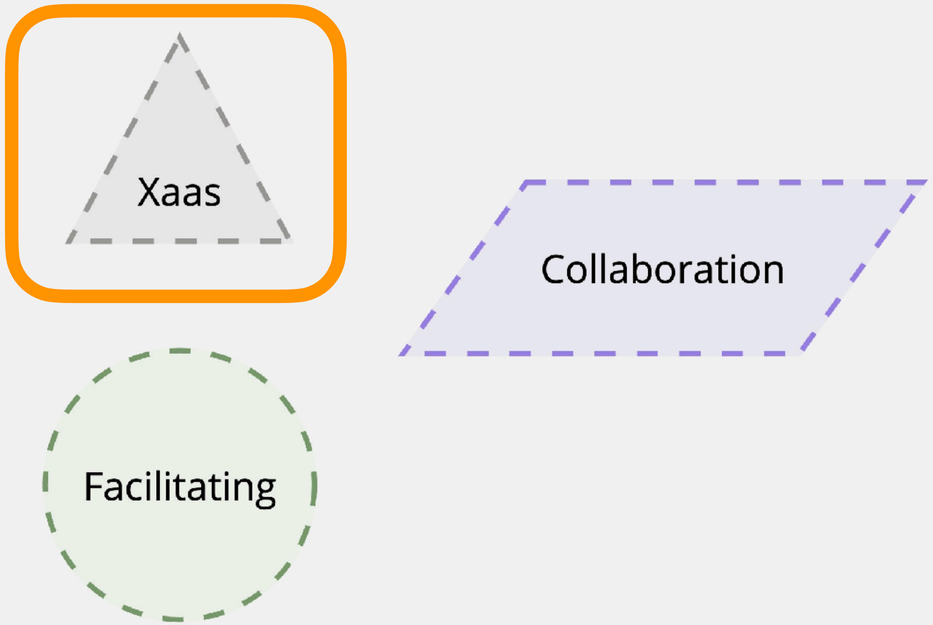


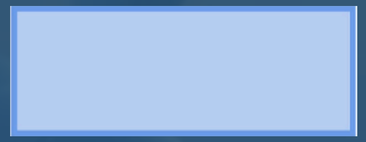


Типы команд



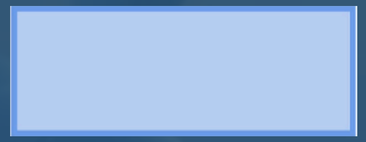
Типы взаимодействия команд





Platform team

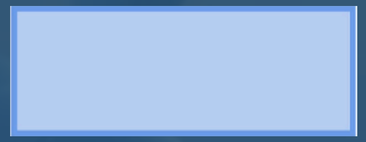
X as a Service



Platform team

X as a Service

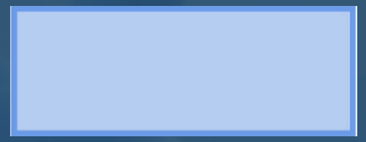
- Уменьшение (!) когнитивной нагрузки



Platform team

X as a Service

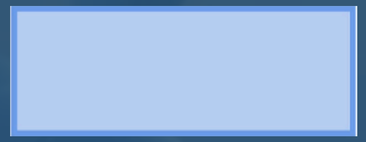
- Уменьшение (!) когнитивной нагрузки
- Понимать потребность клиента



Platform team

X as a Service

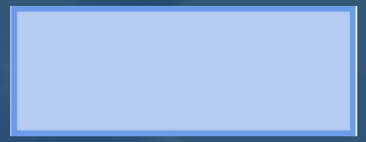
- Уменьшение (!) когнитивной нагрузки
- Понимать потребность клиента
- Создавать возможность обратной связи



Platform team

X as a Service

- Уменьшение (!) когнитивной нагрузки
- Понимать потребность клиента
- Создавать возможность обратной связи
- Определять границы обслуживания



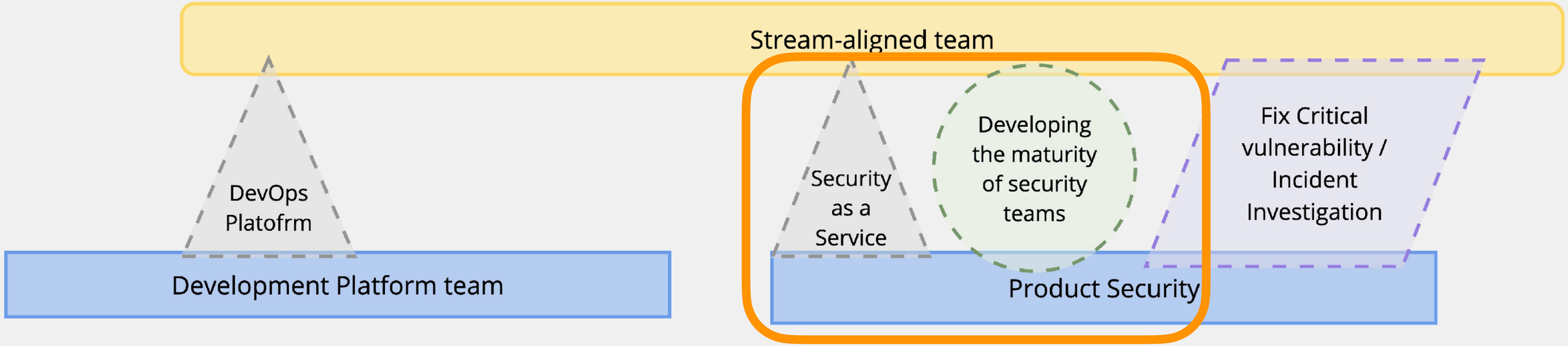
Platform team

X as a Service

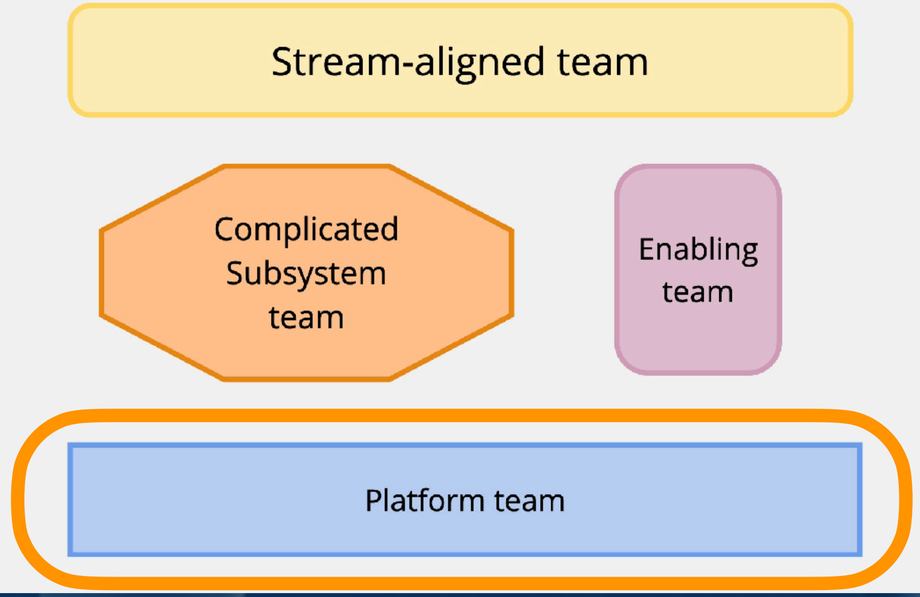
- Уменьшение (!) когнитивной нагрузки
- Понимать потребность клиента
- Создавать возможность обратной связи
- Определять границы обслуживания
- Отвечать за сервис

AppSec - X as a Service

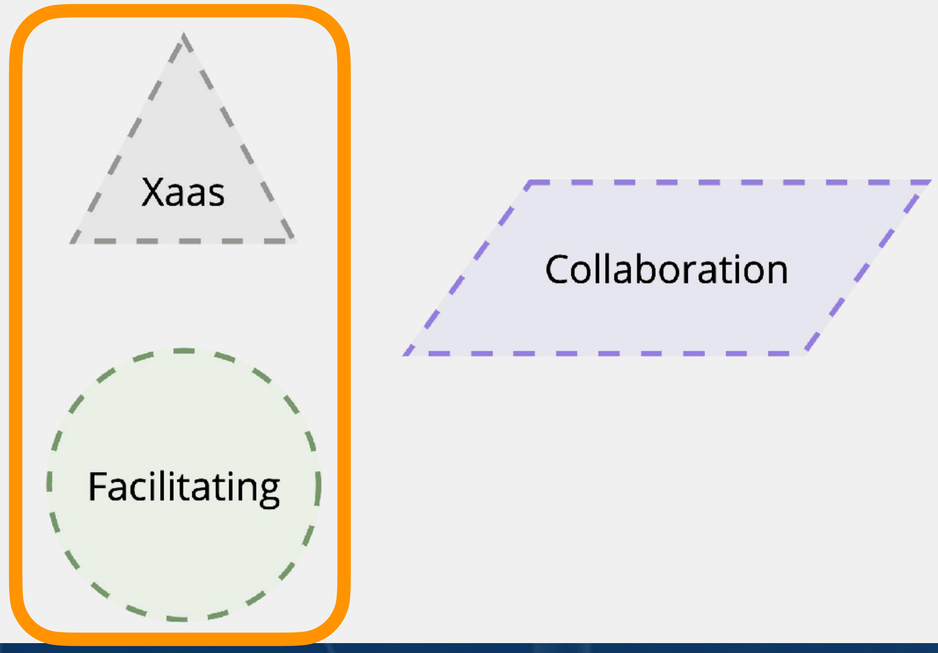
Activity	Team	Type of interaction
Bug Bounty	AppSec	X as a Service
Security Аудит	AppSec	X as a Service
External Penetration Testing	AppSec	X as a Service
Dynamic Security scanners	AppSec	X as a Service
SAST tools in CI\CD pipeline	AppSec	X as a Service
Security Architecture Review	AppSec	X as a Service
Threat Assessment	AppSec	X as a Service



Типы команд



Типы взаимодействия команд



 Enabling Team

 Facilitating

- Повышение производительности, эффективности, создание новой возможности
- Обнаружение и устранение препятствий
- Фасилитация работает с людьми. Изменения в процессах и инструментах - следствие
- Плохо масштабируется

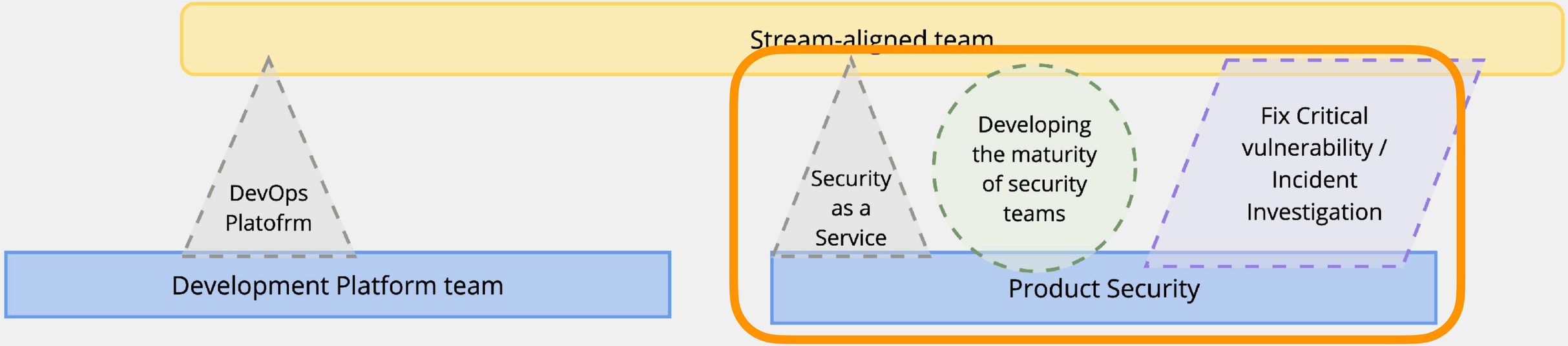
Facilitating

Activity	Team	Type of interaction
Fix existring vulnerability	AppSec	Facilitating
Security Error Budget	AppSec	Facilitating
QA security trainings	AppSec	Facilitating
Secure development awareness	AppSec	Facilitating

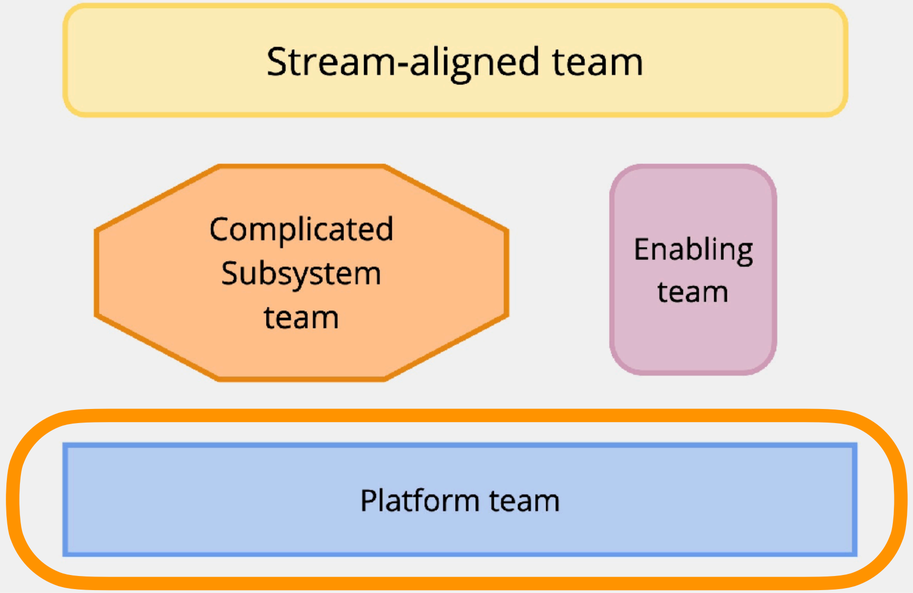
[Продвинутые подходы построения AppSec]

Enabling Team & Security

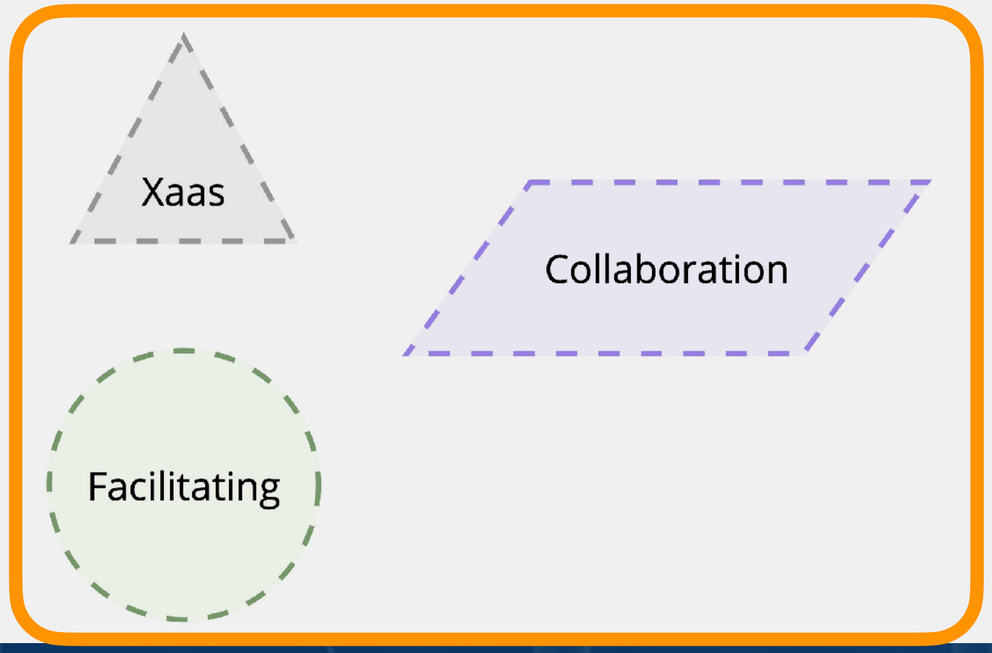
Преодоление закона Конвея



Типы команд



Типы взаимодействия команд

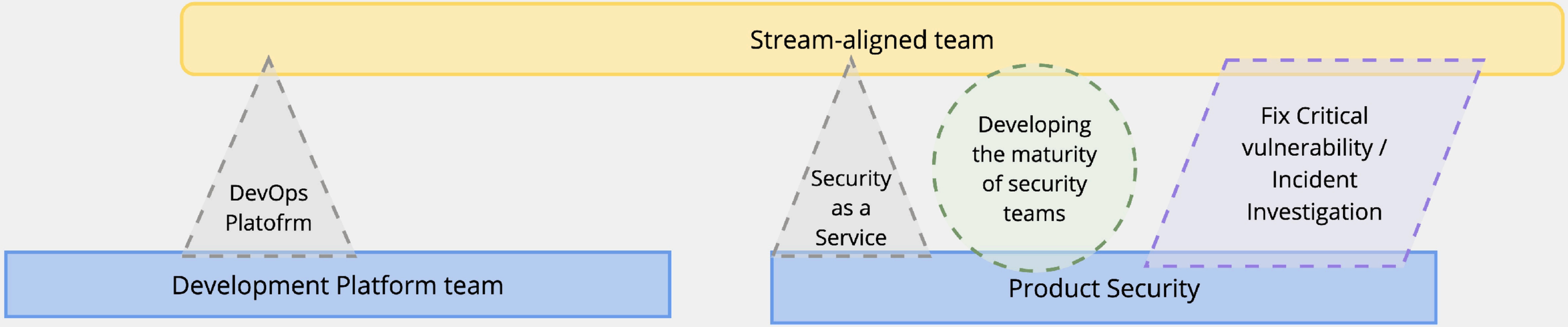


Collaboration

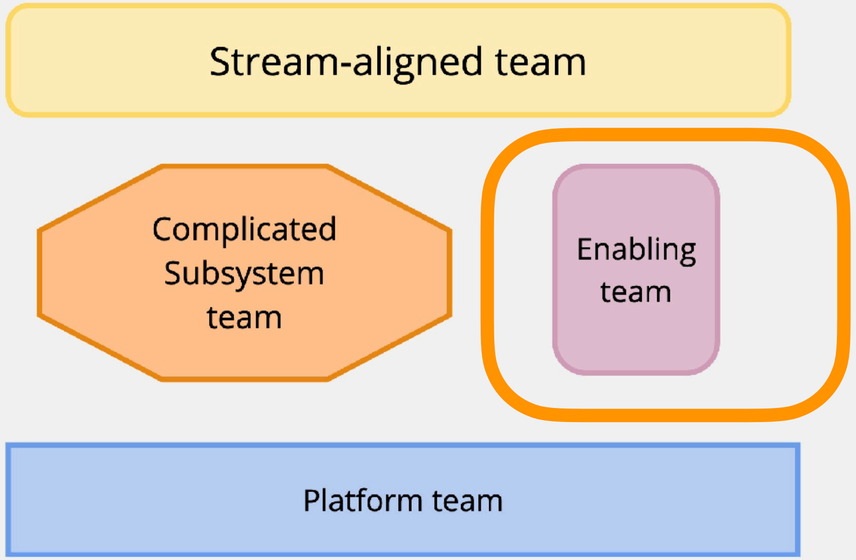
- Быстрое совместное исследование
- Работа над задачей, в которой результат каждой команды важен в равной мере
- Созависимость

Collaboration

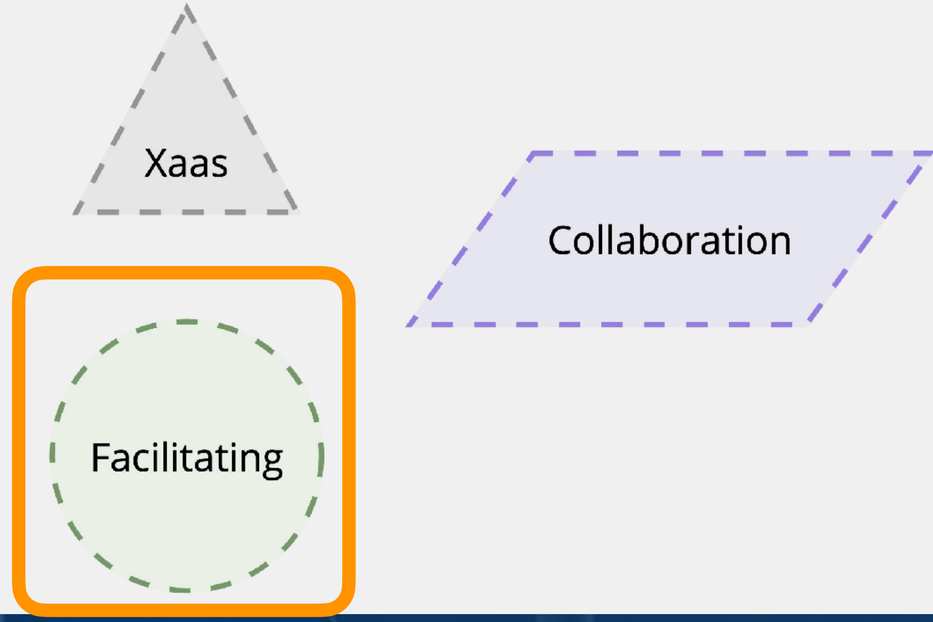
Activity	Team	Type of interaction	
Responding to a Critical Incident	InfraSec	Collaboration	
Fixing critical vulnerabilities	AppSec	Collaboration	
Secure Architecture Solution	InfraSec	X as a Service	Collaboration
Cloud Security	InfraSec	X as a Service	Collaboration
Infrastructure Hardening	InfraSec	X as a Service	Collaboration



Типы команд



Типы взаимодействия команд



Про что сегодня поговорили?

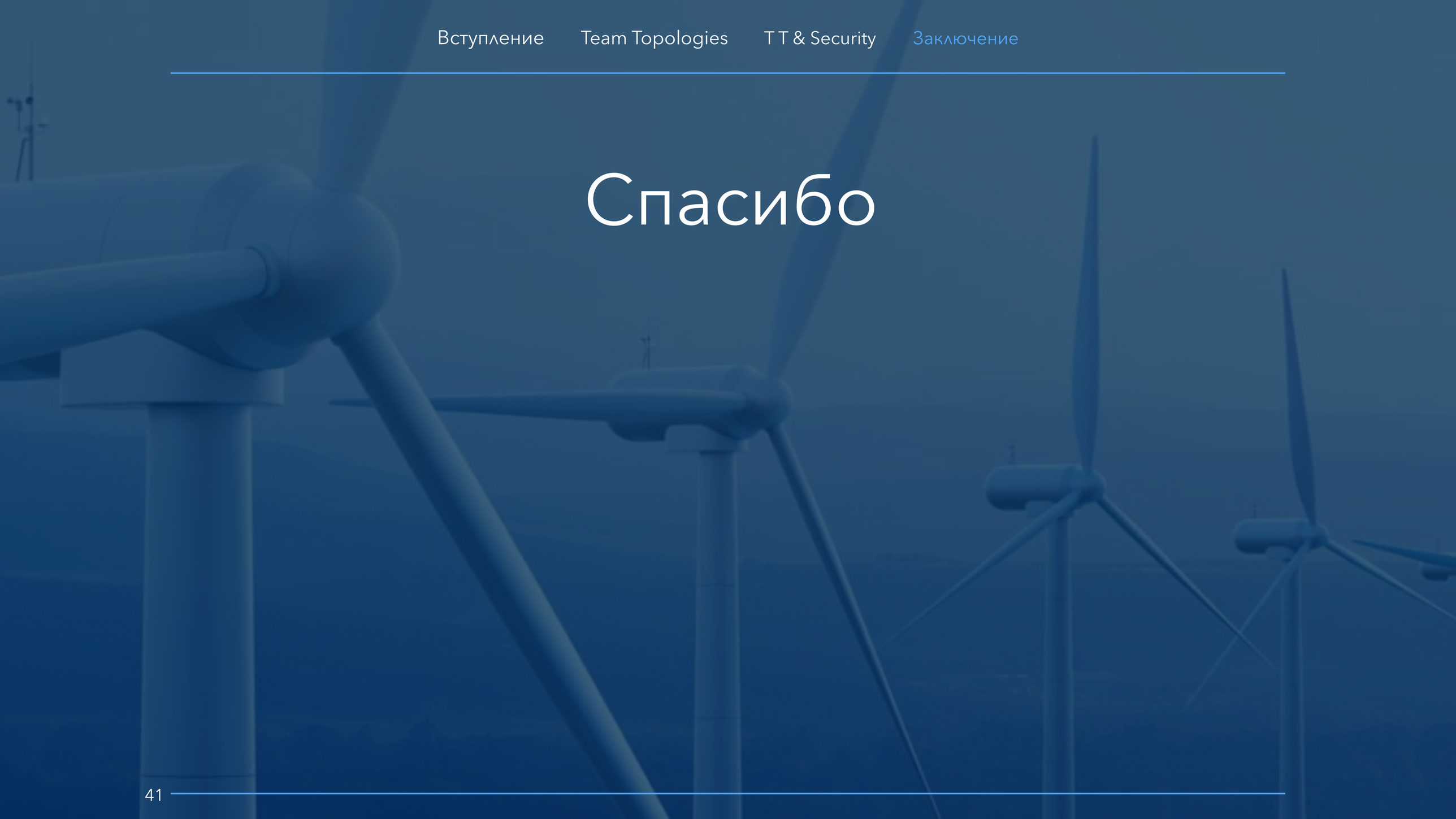
- Конвейер и ИТ
- Team Topologies
  - Подход Team First
  - Закон Конвея
  - Team API
  - 4 типа команд
  - 3 типа отношений
- Требования к качеству сервиса у платформенной команды
- Платформенная команда и зрелость клиента
- TT & безопасность

Итого

- Team Topologies - инструмент структурирования связей команд
- Team Topologies - инструмент создания общих требований к работе платформенных команд
- Team Topologies - набор

Reference

- Team Topologies: Organizing Business and Technology Teams for Fast Flow (book).
- Teamtopologies.com
- DevOps Topologies
- Getting started with Team Topologies - infographic
- Team Topologies in a nutshell - infographic
- Team API template
- Thinnest Viable Platform examples
- Agile Security (book)



Спасибо