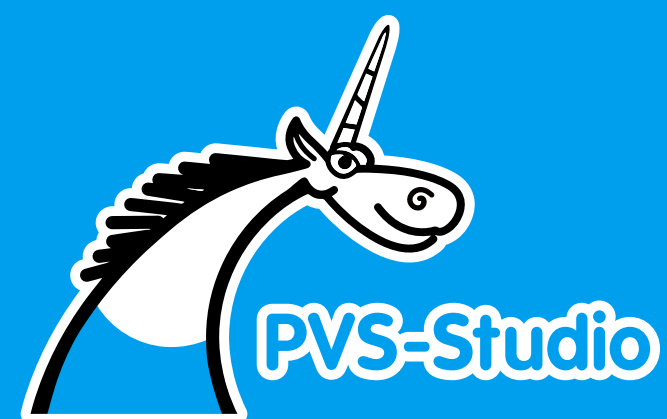


Как это происходит на практике



- **Выявление недостатков и уязвимостей:**
 - Внутреннее сканирование (SAST, SCA, DAST)
 - Внешнее сканирование (пентест, багбаунти)
 - Запрос клиента на исправление багов
- **Запросы на дополнительную функциональность:**
 - Запрос клиента на реализацию новой функции
 - Внутренний запрос (новая функция для повышения конкурентоспособности на рынке)
 - Запрос рынка («у всех есть эта функция, а у нас до сих пор нет»)
- **Снижение количества недостатков**
 - Метрики (сколько уязвимостей было, сколько стало, технический долг)
- **Оперативное устранение выявляемых уязвимостей**
 - SLA (Service Level Agreement) - соглашение об уровне обслуживания, определяющее параметры предоставляемой услуги между заказчиком и исполнителем. Определяет сроки исправления обнаруженной уязвимости в зависимости от ее критичности

■ Инструменты:

- ASPM (Application Security Posture Management, Управление состоянием безопасности приложений) – используется для оркестрации и корреляции уязвимостей, а также для внедрения политик безопасности, управления рисками
- Тикет-трекеры – нужны для планирования задач и отслеживания их выполнения. Объединяют в себе отслеживание запросов на новую функциональность и на исправление недостатков ПО.

Как AppSec.Hub помогает выполнять данные требования

