



РИСКИ САМОСТОЯТЕЛЬНОЙ РАЗРАБОТКИ ФИНАНСОВЫХ ПРИЛОЖЕНИЙ ИНСТРУМЕНТЫ ИХ МИНИМИЗАЦИИ

Рустэм Хайретдинов
Appercut Security

- 👉 **Несистемные требования по безопасности приложений**
Упор на функционал и нагрузку, игнорирование стандартов
- 👉 **Службы ИБ в разработке не участвуют**
Привлекаются только к расследованиям инцидентов
- 👉 **Упрощенный процесс разработки**
Изменения идут непрерывно, код правится вместо выпуска патчей
- 👉 **Используются закрытые платформы**
SAP, Oracle, MS Dynamix, 1C, Lotus, Directum, Quorum ...

КЛАССИЧЕСКИЙ ПОДХОД К АУДИТУ БИЗНЕС-ПРИЛОЖЕНИЙ

RRO: может находить
сложные уязвимости

CONTRA: долгий,
дорогой и
сложный процесс



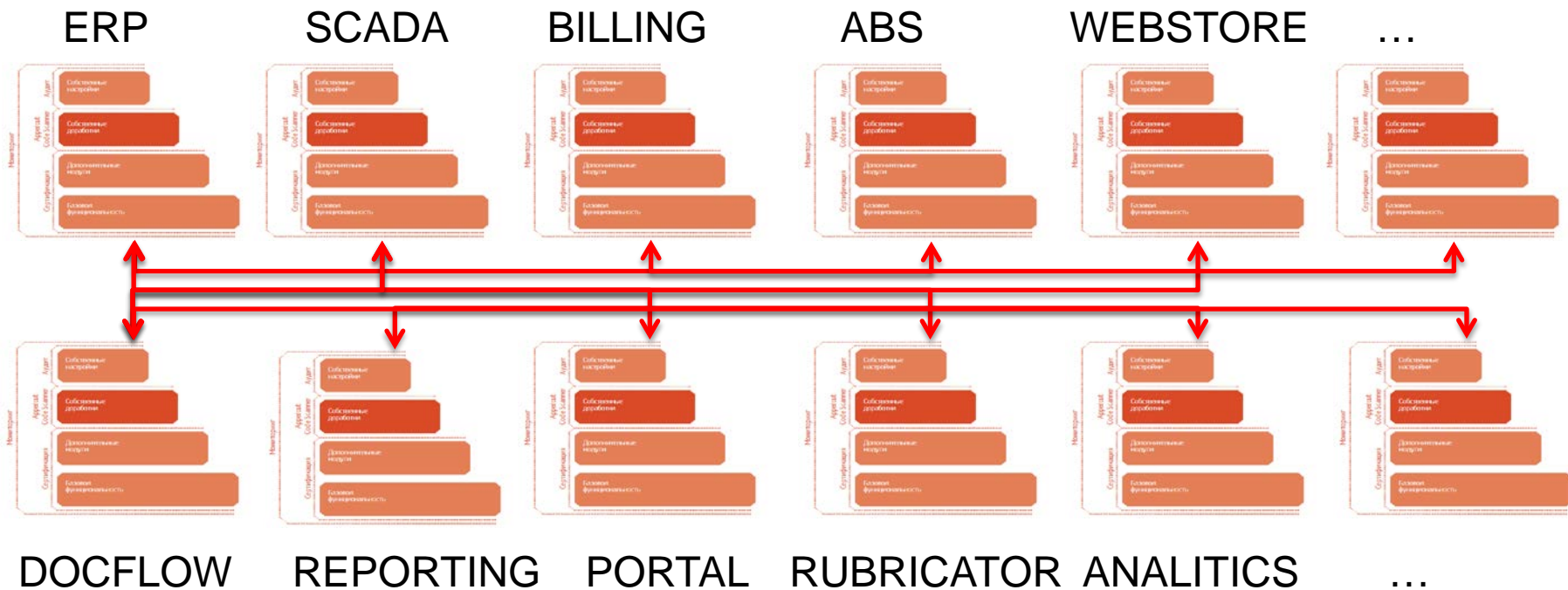
Настройки

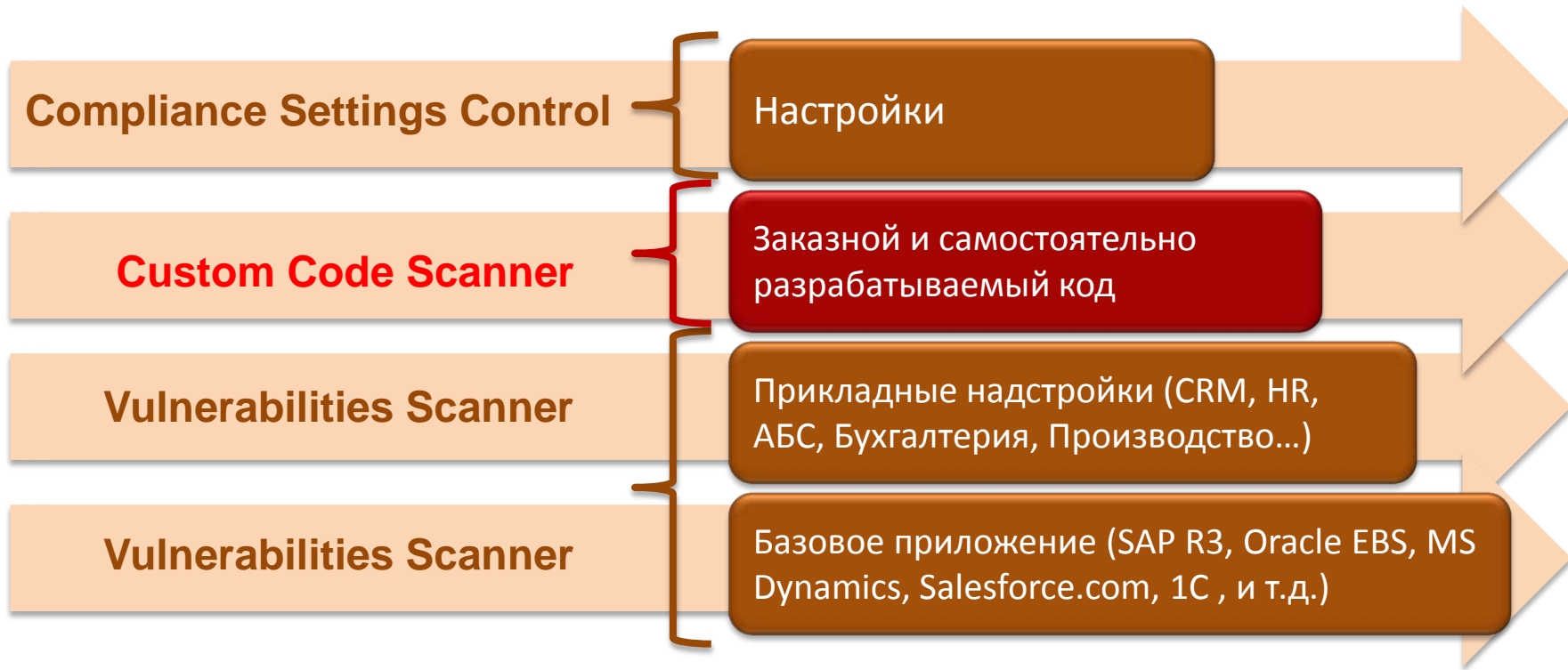
Заказной и самостоятельно
разрабатываемый код

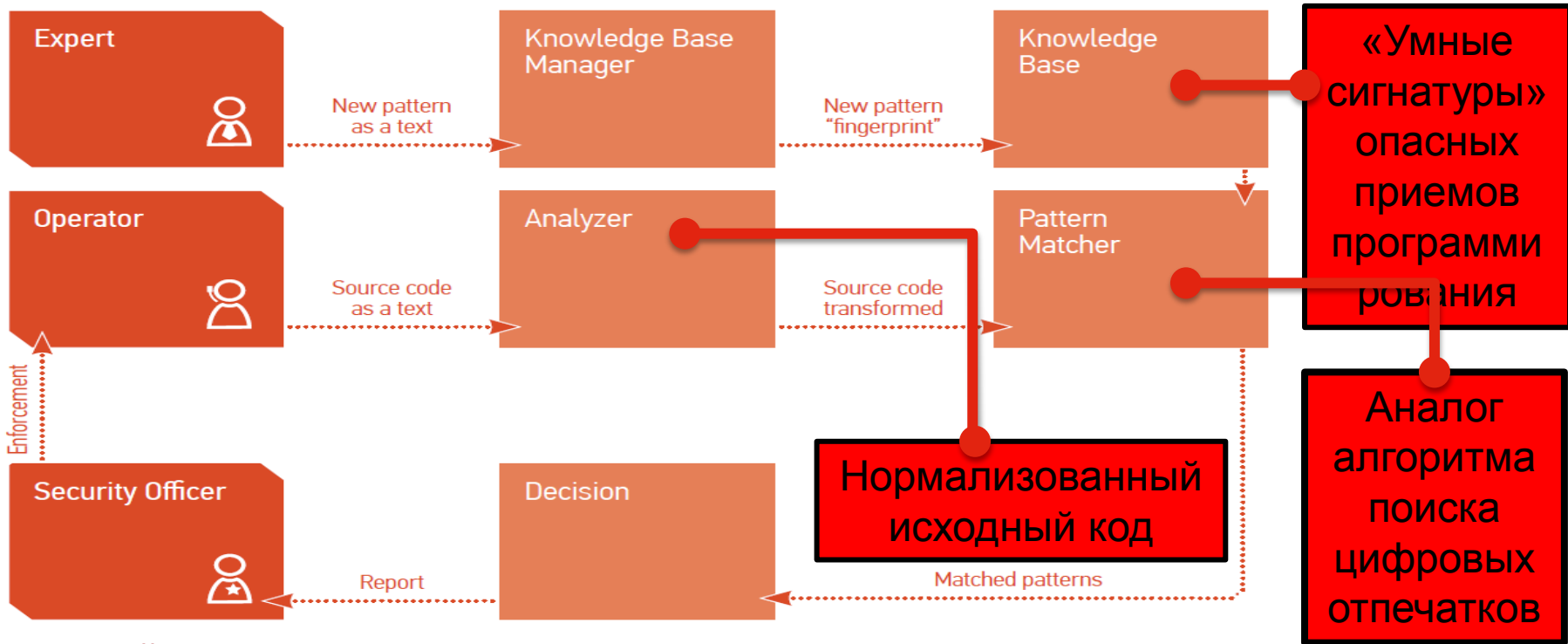
Прикладные надстройки (CRM, HR,
АБС, Бухгалтерия, Производство...)

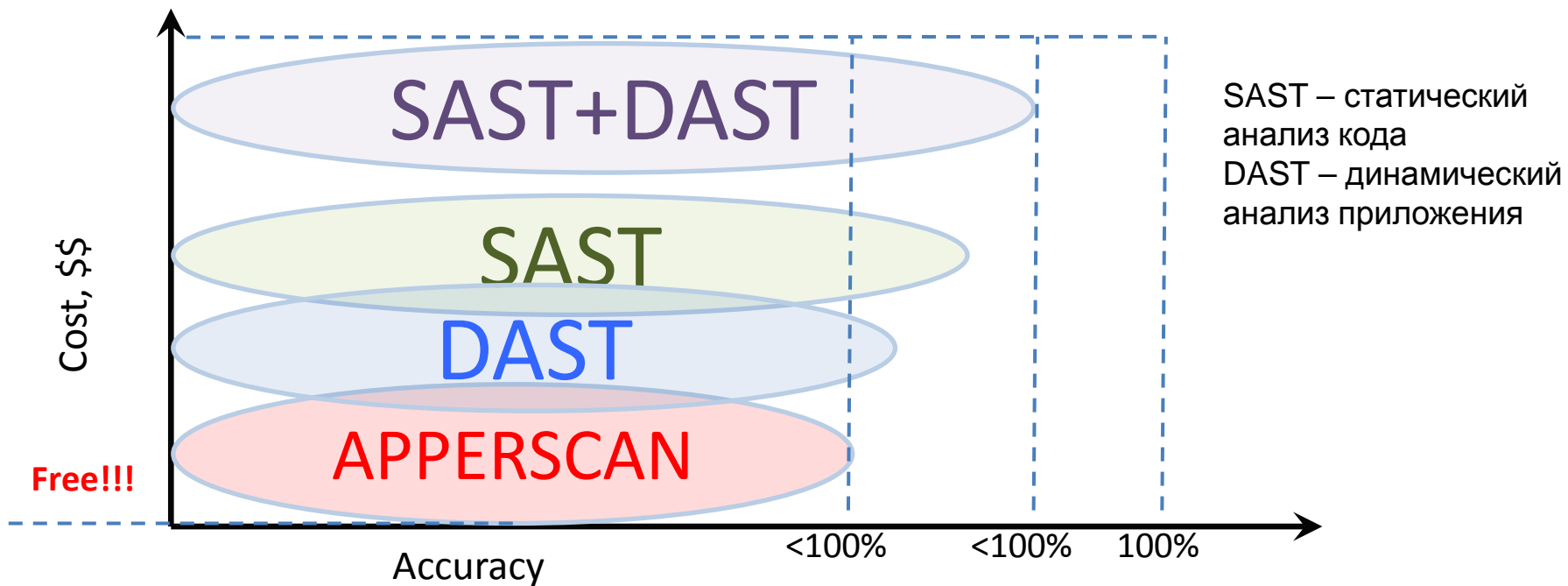
Базовое приложение (SAP R3, Oracle EBS, MS
Dynamics, Salesforce.com, 1С , и т.д.)

ЧТО ДЕЛАТЬ, ЕСЛИ У ВАС ТАК?



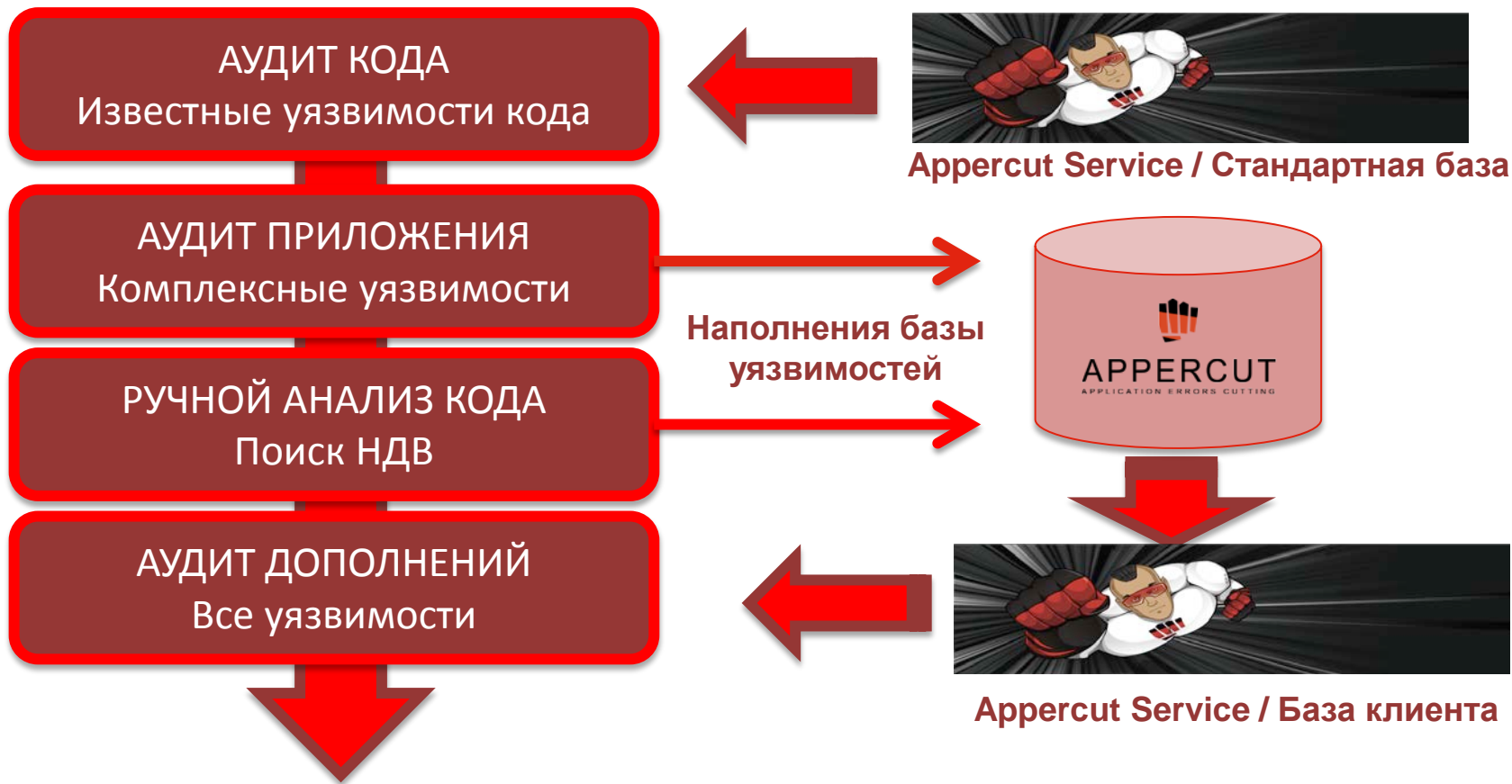


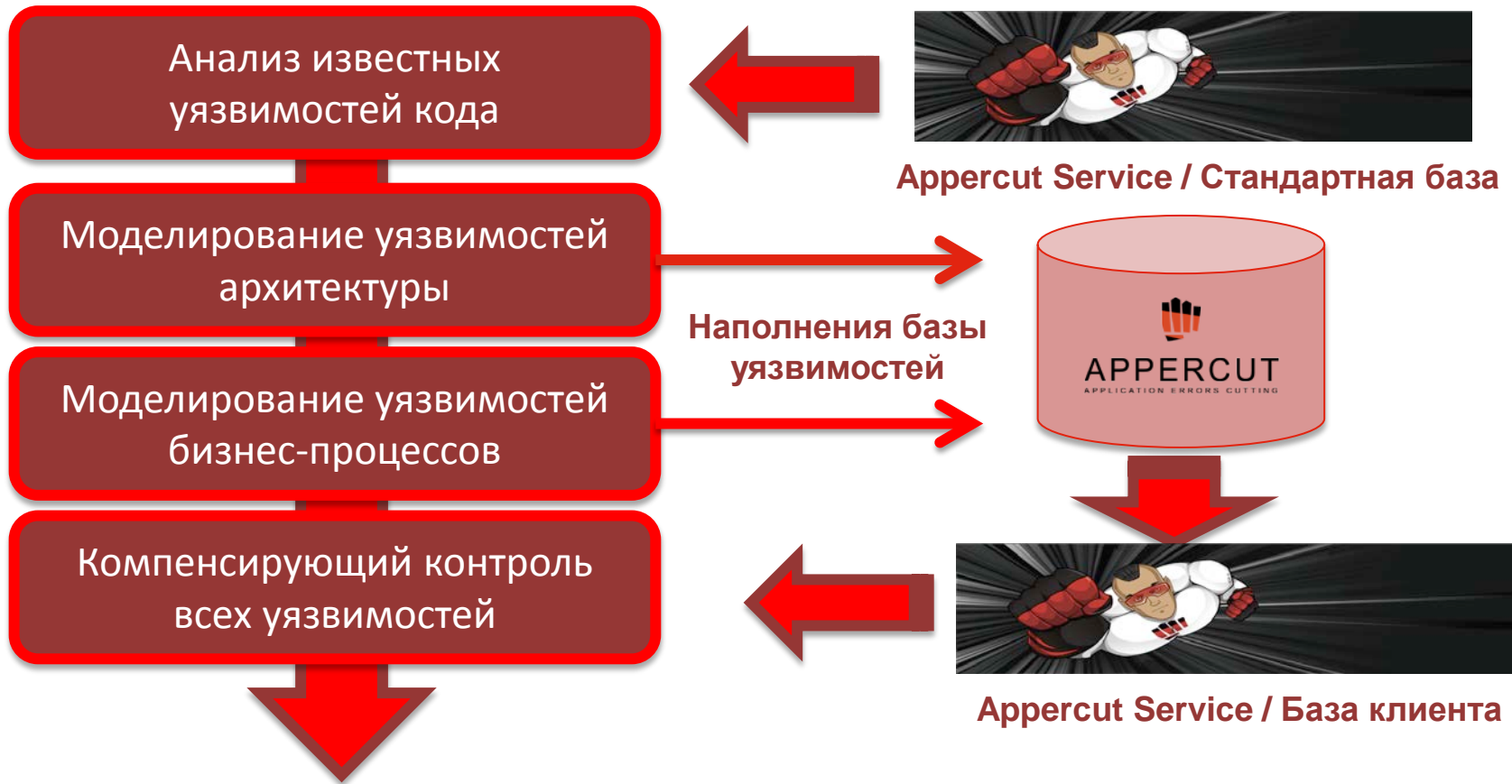




- ❏ Не предполагается встраивание в процесс разработки
- ❏ Не предполагается участие программистов
- ❏ Аудируется любое количество приложений
- ❏ Возможность добавлять пользовательские уязвимости
- ❏ Реализация в виде веб-сервиса (SaaS, Private Cloud)

- 👉 Традиционные средства разработки: Java, JavaScript, PHP, Ruby, Cobol, C++, T-SQL, Visual Basic, Delphi, C#, ASP, Objective C, Python...
- 👉 Традиционные бизнес-платформы: ABAP4 (SAP), PL/SQL (Oracle), LotusScript (IBM Lotus Notes), Microsoft Dynamix (X++), 1C ...
- 👉 Проприетарные языки: SAS Script, x-Script, z-Script (БОСС), (Directum), Atlantis (Quorum)
- 👉 Любая платформа на заказ (нормализатор + 10 TOP-уязвимостей) – 1 месяц





ВОПРОСЫ, ПОЖАЛУЙСТА!



APPERCUT
APPLICATION ERRORS CUTTING

Рустэм Хайретдинов

Appercut Security

sales@appercut-security.com

+7(903)961-7312

www.appercut.com

Уральский форум, Магнитогорск, 14.02.2013