

A top-down view of a desk with a red coffee cup, a blue pen, and a laptop keyboard. The desk is light-colored wood. The coffee cup is red with a white interior. The pen is blue with silver accents. The laptop keyboard is dark grey.

ATTACK KILLER

Комплексная защита
веб-приложений

Андрей Милованов

Коротко о нас



Используют наши технологии



Russia & CIS:



Правительство Санкт-Петербурга
Комитет по информатизации и связи



Комитет по информатизации
г. Тюмени



Министерство обороны Российской Федерации



Сахалинский областной центр информации



Worldwide:

AUTOMATTIC



Acronis



ВЕБ-УГРОЗЫ В ЦИФРАХ

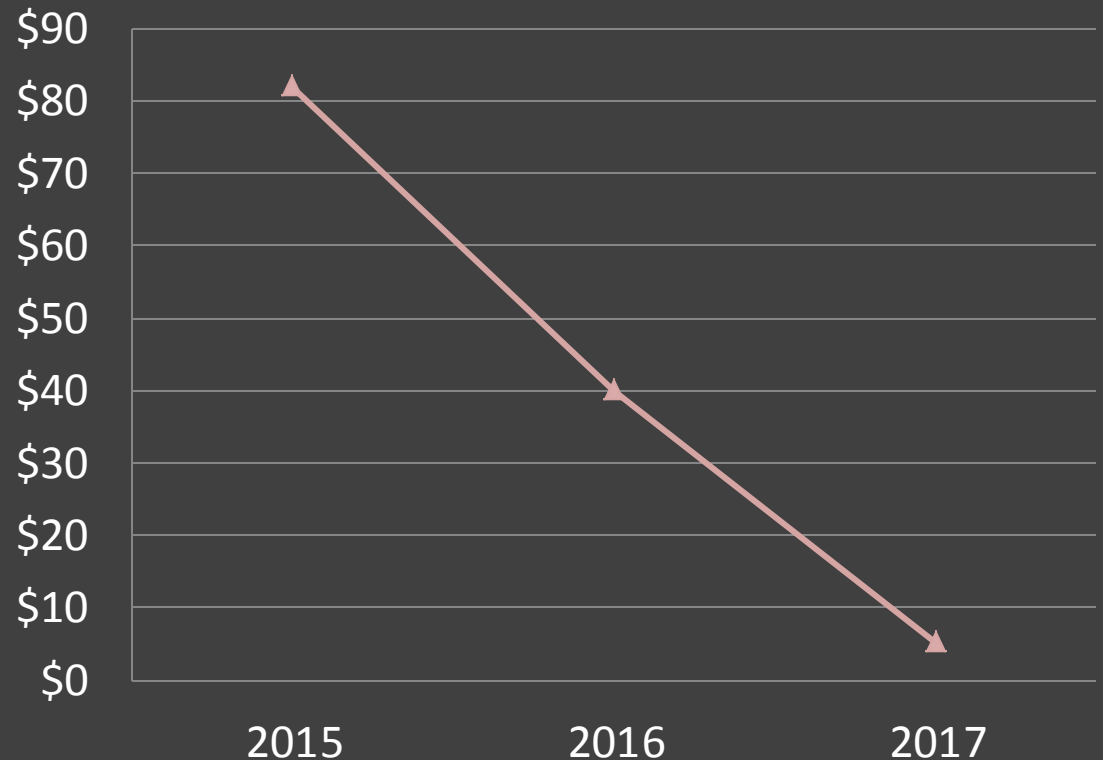
84% атак
совершаются
комплексно:
DDoS+хакерский
взлом

Каждый 3-й
ресурс содержит
давно известные
уязвимости

Рост числа атак на
50-70% в год

Атаки становятся дешевле,
число их растет

Стоимость DDoS-атаки



Инциденты :
как это было и к
чему привело



Рособрнадзор & NoraQ

Сценарий:

Хакер получил доступ к БД ведомства с помощью SQL-инъекции.

В форму для проверки подлинности дипломов были введены некорректные данные. Это привело к SQL-инъекции, благодаря чему хакер смог получить доступ к БД и изучить ее структуру, а после с помощью скрипта на Python скачать данные.

Последствия:

Прямой доступ к данным по дипломам, ПД 14 млн россиян



Нефтяная компания: integration debugging

Сценарий:

Проведена сквозная интеграция БП печати накладной на отгрузку и пропуска на транспорт.

Печать документов потребовала отладки. Для этого разработчики сделали тестовый процесс, не требующий проверки.

Сотрудники смогли печатать пропуска на авто без накладных и вывозить товар со склада

Последствия:

**Значительные финансовые
потери**

Заведены уголовные дела



Retailer:

когда все в одних руках

Сценарий:

Разработкой приложений занималась внутренняя команда.

Сильная кастомизация кода, без документации – полная завязка БП компании на конкретных людей.

После увольнения архитектор решил «свести счеты» - зная архитектурные изъяны сервиса

Последствия:

Полная остановка сервиса по приему платежей, по всей стране

Недополученная прибыль



Подход к управлению ИБ



WAF

Защита веб-приложений

Правила и политики безопасности

Reporting

Агрегированная отчетность

CORE

Единая панель управления



Anti DDoS

Доступность приложений

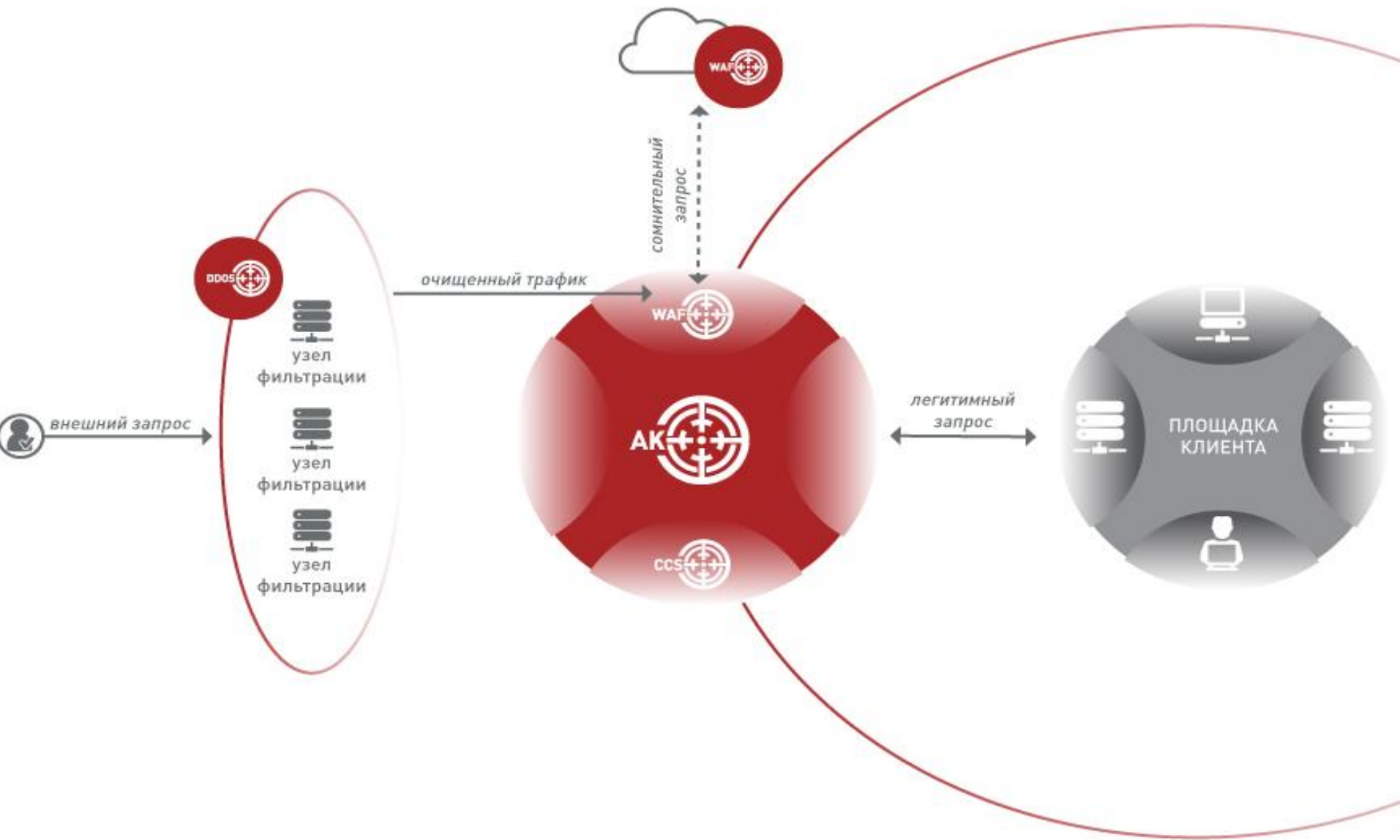
CCS

Анализ исходного кода

API

Интеграция с внешними системами

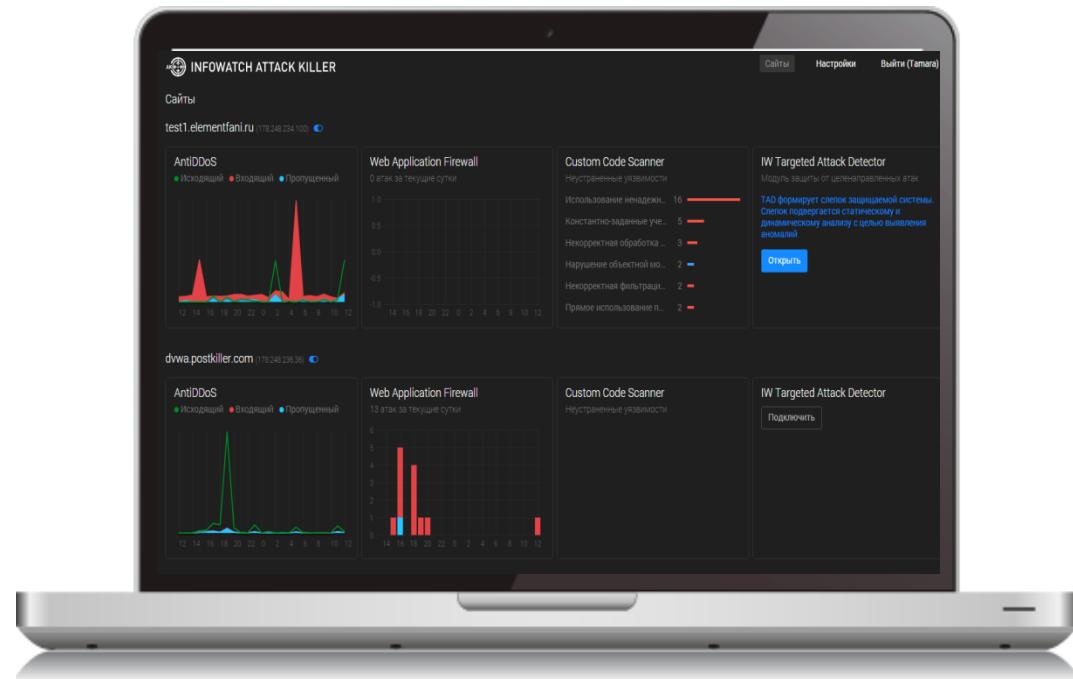
Общая схема внедрения



Единый веб-интерфейс

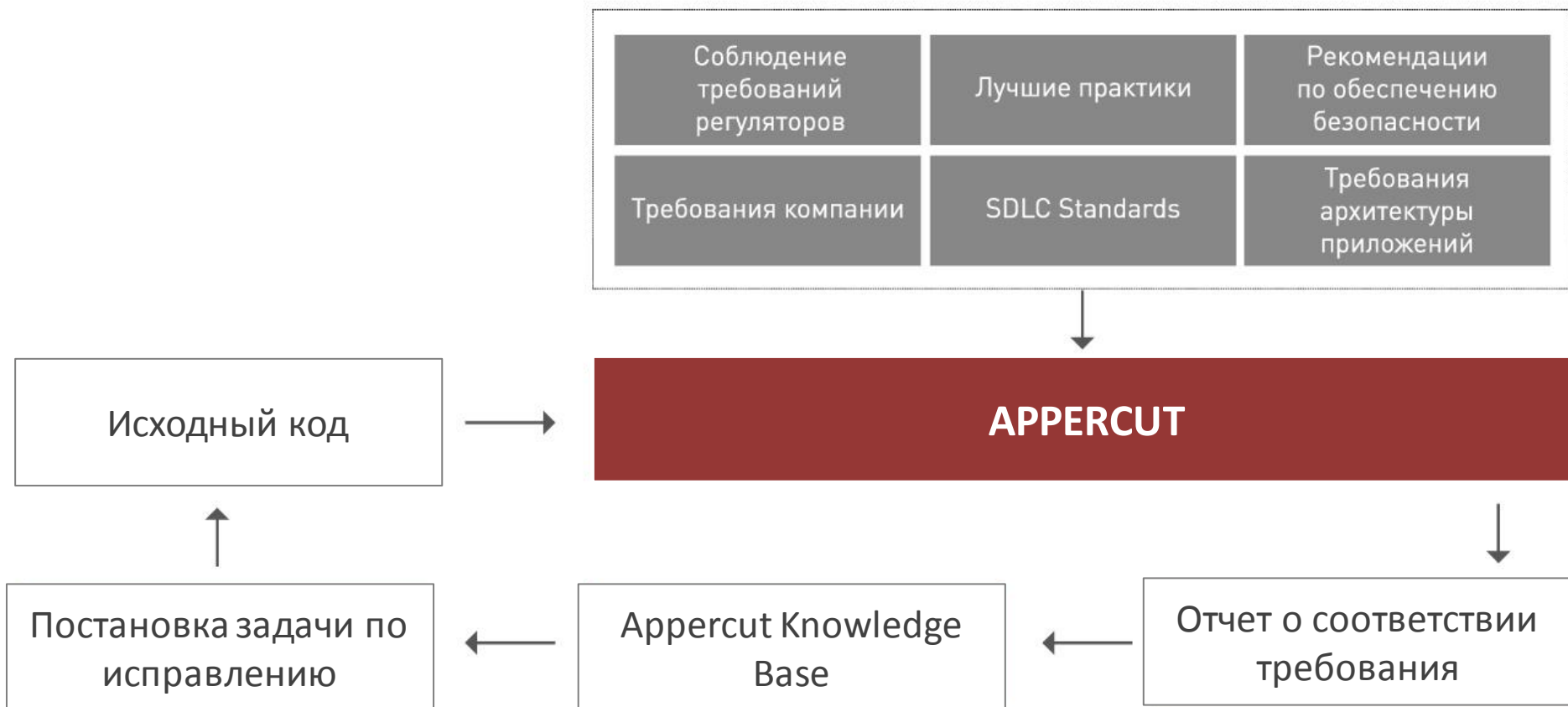


- Одно решение для защиты от любых веб-угроз
- Модульная схема подключения
- Единый веб-интерфейс и единые отчеты
- Машинное обучение
- Синергия технологий





Appercut - система автоматизированного контроля исходного кода



Attack Killer:

ЛУЧШИЕ ТЕХНОЛОГИИ ПОД УПРАВЛЕНИЕМ ИИ



Непрерывная безопасность

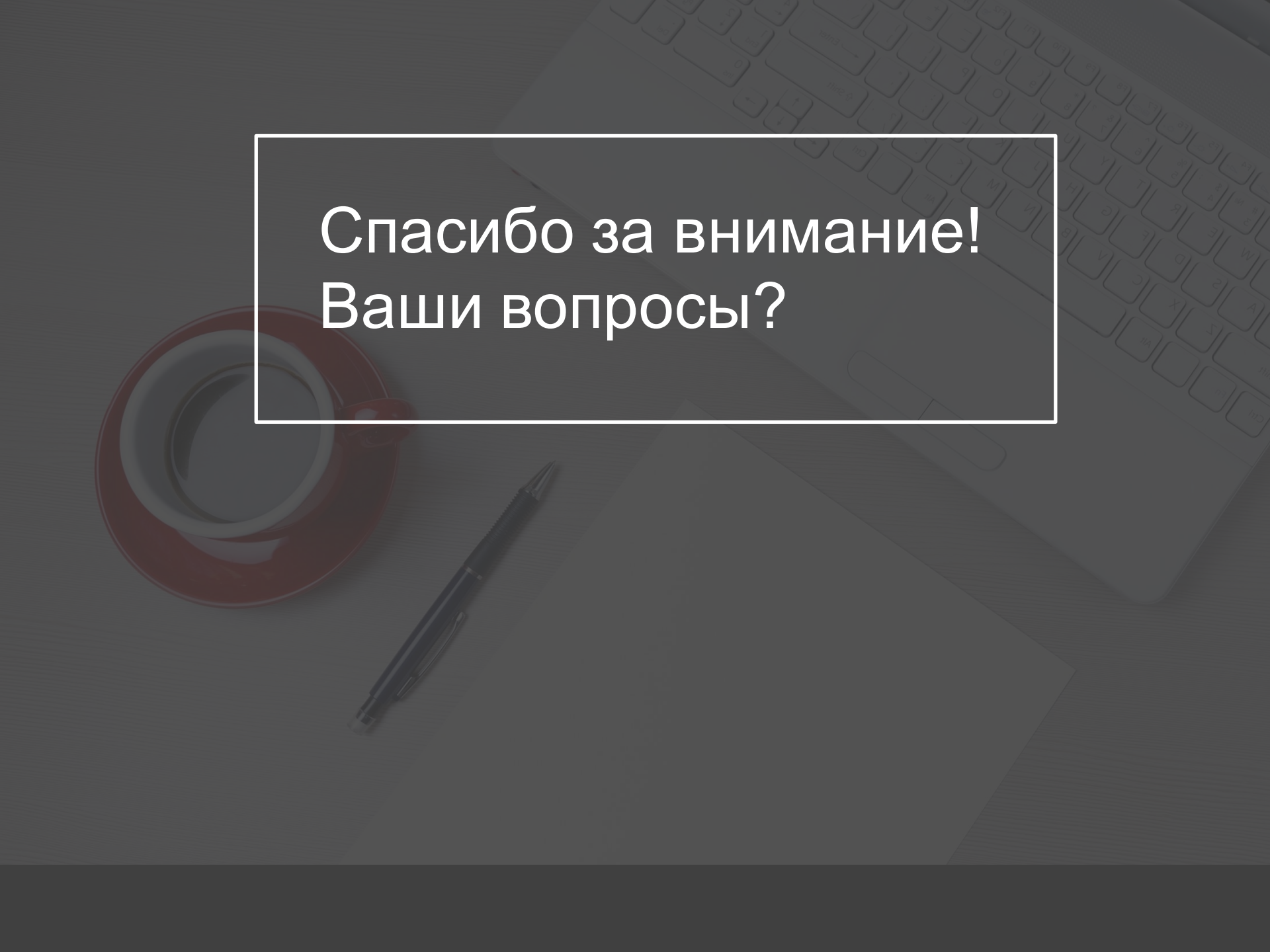
Активная защита при регулярных изменениях, нивелирующая человеческий фактор

Управление через единый веб-интерфейс

Наглядные графики и отчеты о попытках атак на всех уровнях защиты

Модульная схема подключения: начните с необходимого

Простое подключение других модулей «галочкой» через веб-интерфейс



Спасибо за внимание!
Ваши вопросы?