АНТИФИШИНГ

Shift-Left Security: как подружить безопасность и продуктовые команды

blog.antiphish.ru

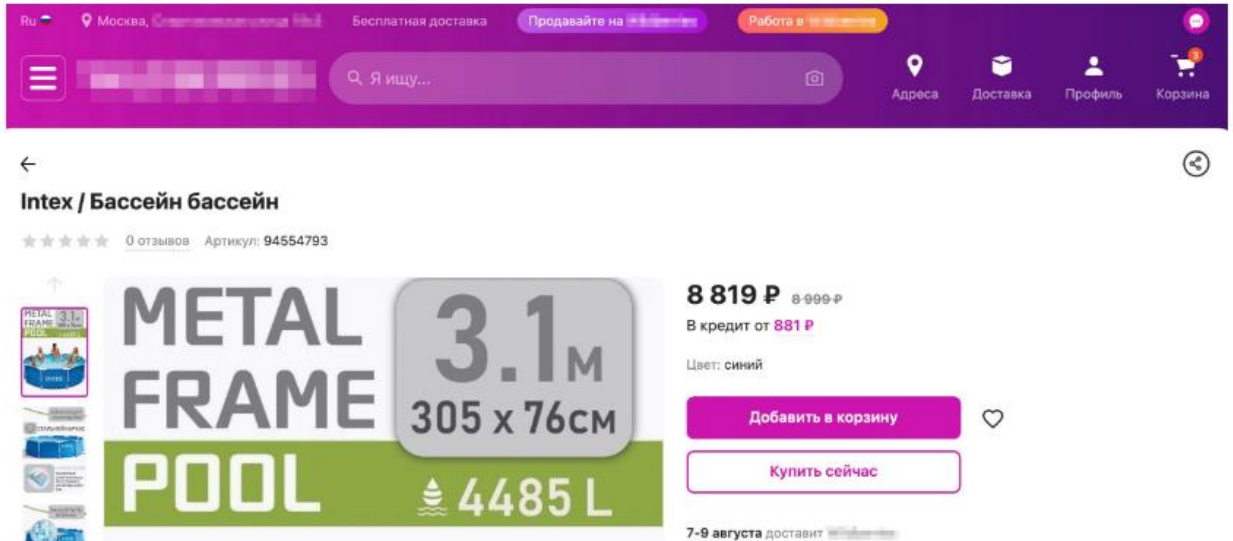
t.me/antph

Киберкампании

Обнаружена мошенническая кампания, для проведения которой используется популярный маркетплейс.

Схема действий мошенников

1. Мошенники выкладывают на официальный сайт известного маркетплейса несколько товаров. Это может быть все, что угодно: от дачного бассейн до смартфона. Преступники представляются разными продавцами, но используют один и тот же номер.

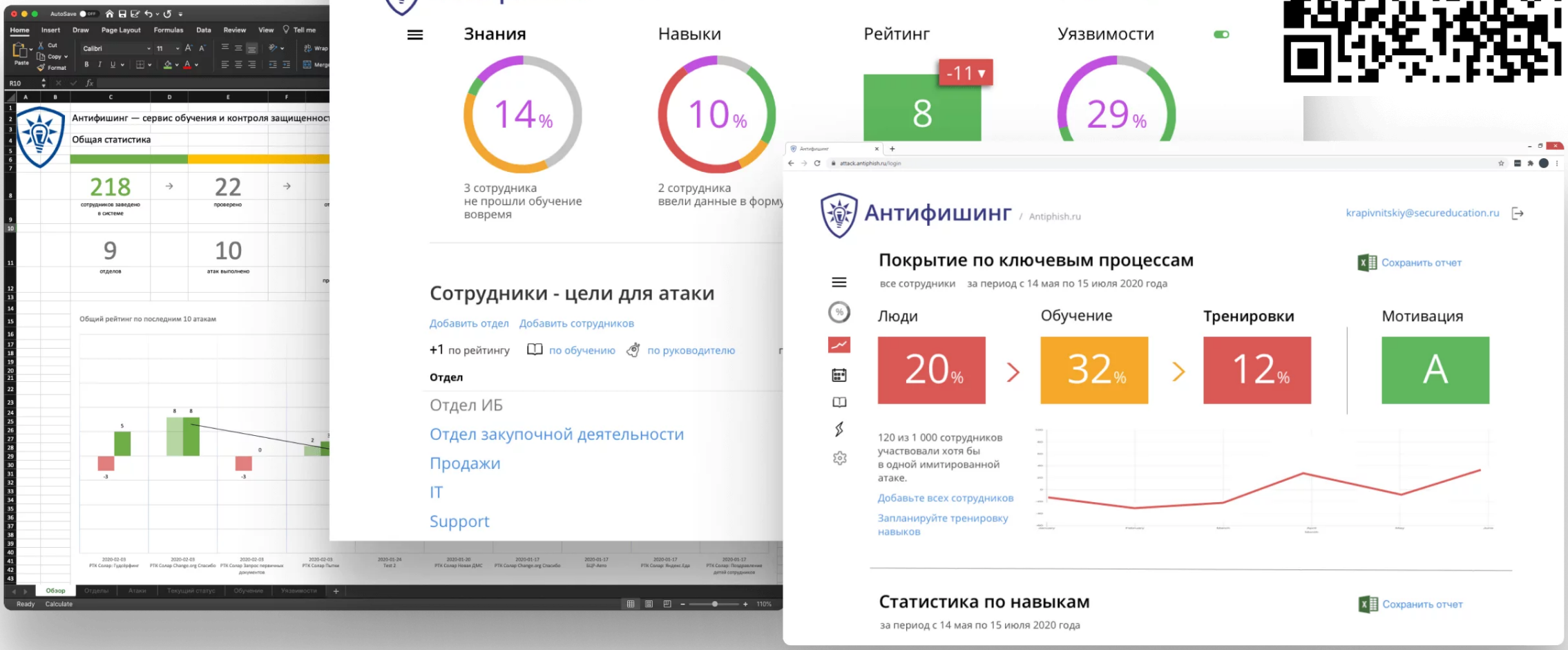


Андрей Жаркевич
редактор

Артемий Богданов
технический директор

Сергей Волдохин
выпускающий редактор

Антифишинг для всех сотрудников



Информационная безопасность

26.01.2022, 00:47

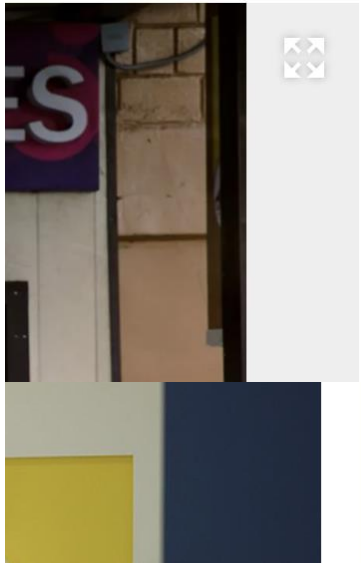
Вирус взял подработкой

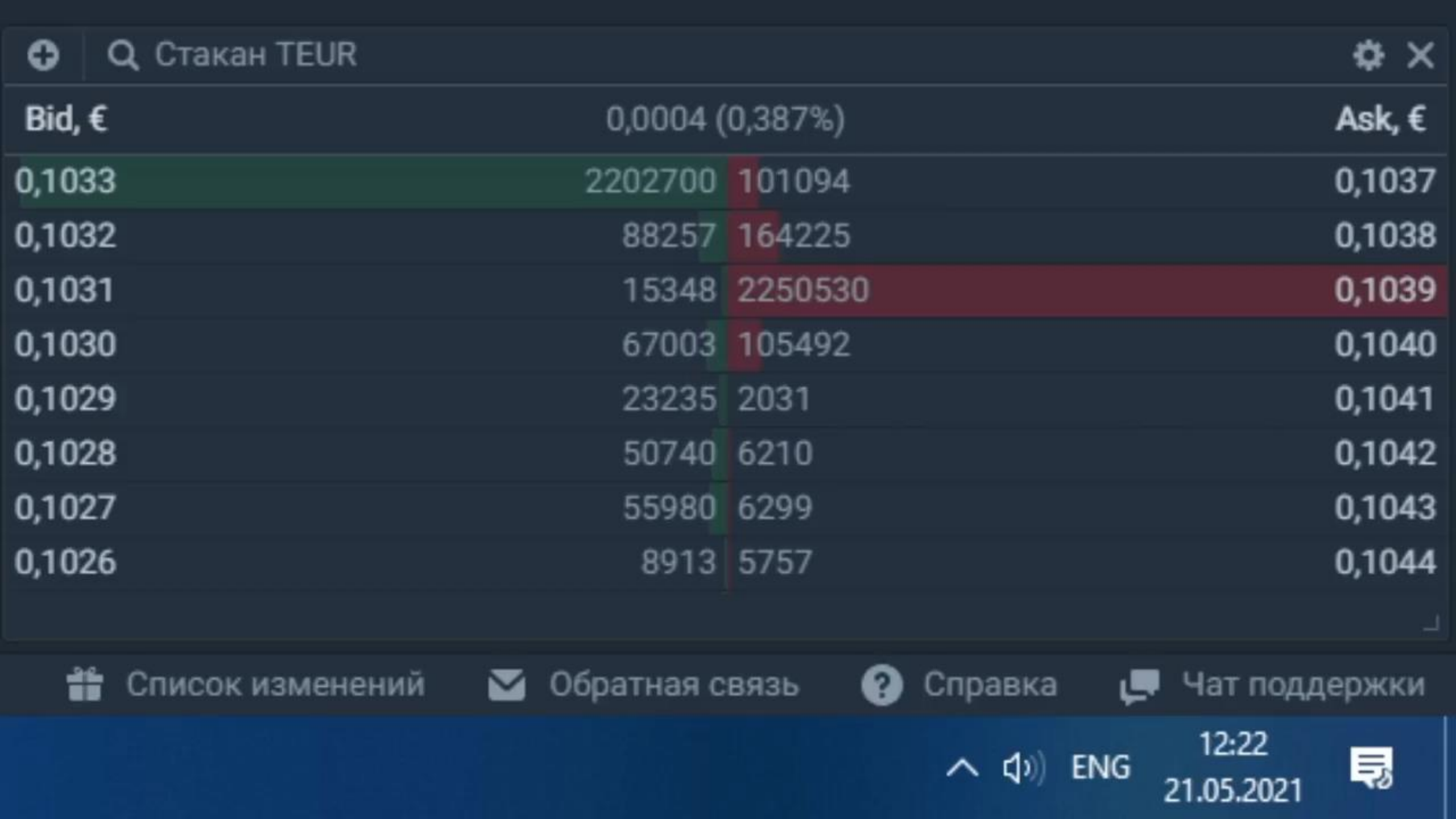
В доработанных модулях 1С нашли вредоносный код

Данные нескольких десятков компаний были украдены через вредоносный код в модулях 1С, обнаружили в RTM Group. По ее данным, он встраивался в программное обеспечение (ПО) во время доработки модулей у программистов на аутсорсинге. В самой 1С утверждают, что не сталкивались с такими случаями, но, чтобы избежать злоупотреблений, предлагают клиентам обращаться к официальным сертифицированным партнерам. Подобные вещи не всегда происходят умышленно, уточняют эксперты, заражен может быть компьютер самого исполнителя.

нное

/головное дело
и регистрировались
о, а затем уже под
изитам. Тем не менее
ошеннические схемы
ыстром росте, отсюда




Стакан TEUR
Bid, €
0,0004 (0,387%)
Ask, €
0,1033 2202700 101094 0,1037
0,1032 88257 164225 0,1038
0,1031 15348 2250530 0,1039
0,1030 67003 105492 0,1040
0,1029 23235 2031 0,1041
0,1028 50740 6210 0,1042
0,1027 55980 6299 0,1043
0,1026 8913 5757 0,1044
Список изменений
Обратная связь
Справка
Чат поддержки
ENG
12:22
21.05.2021

Doublesharp 2 апреля 2021 в 18:49

Путаница зависимостей. Как я взломал Apple, Microsoft и десятки других компаний

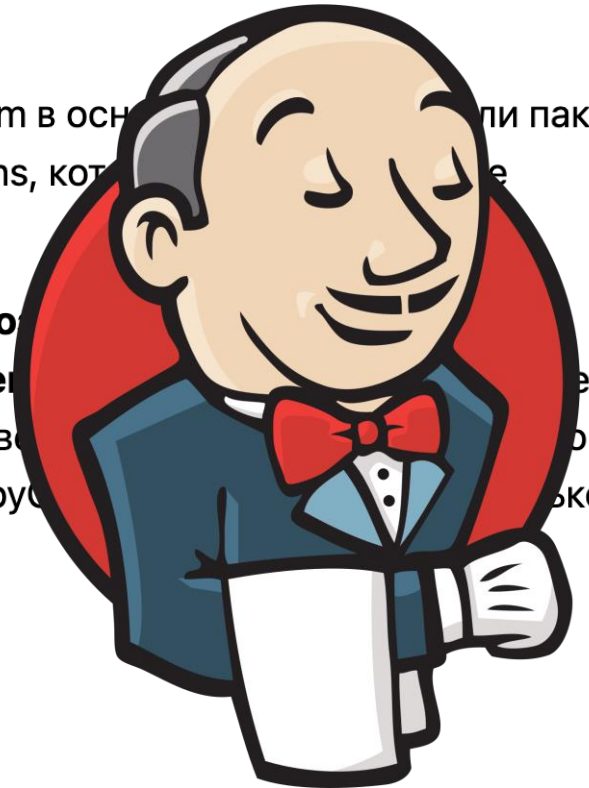
Код предназначался для внутреннего использования в PayPal, и в его файле package.json, по-видимому, содержалась смесь публичных и частных зависимостей — публичные пакеты от npm, а также имена непубличных пакетов, скорее всего, размещённых внутри PayPal. В то время этих имён не было в публичном реестре npm.

https://habr.com/ru/company/skillfactory/blog/550380/

```
"dependencies": {
  "express": "^4.
  "dustjs-helpers
  "continuation-l
  "pplogger": "^0
  "auth-paypal":
  "wurfl-paypal":
  "analytics-payp
}
```

При загрузке зависимостей менеджеры пакетов npm, pip и gem в осн ли пакеты из основных общедоступных репозиториев NPM, PyPI и RubyGems, кот е приоритетными.

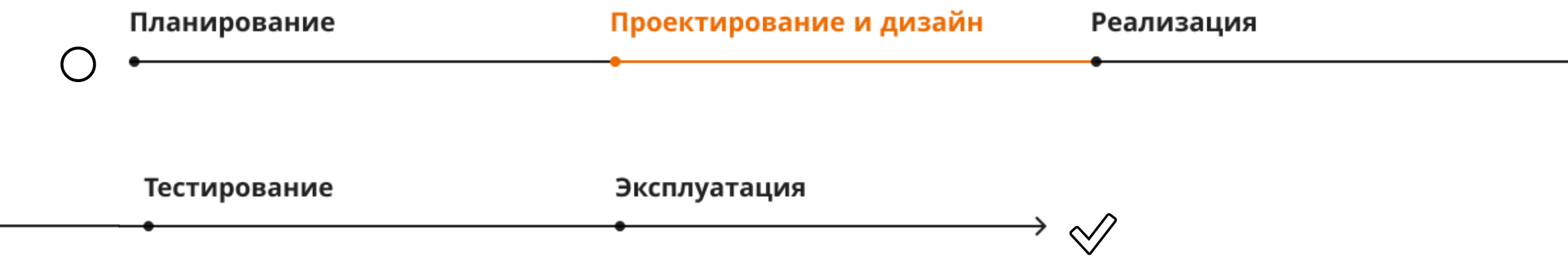
Присутствие похожих пакетов с такими же именами в репо
игнорировалось без отображения предупреждений и сбое е
администраторов. В PyPI на приоритет загрузки влиял номер в ория была загружена самая последняя версия пакета). В NPM и Ruby ько от репозитория.



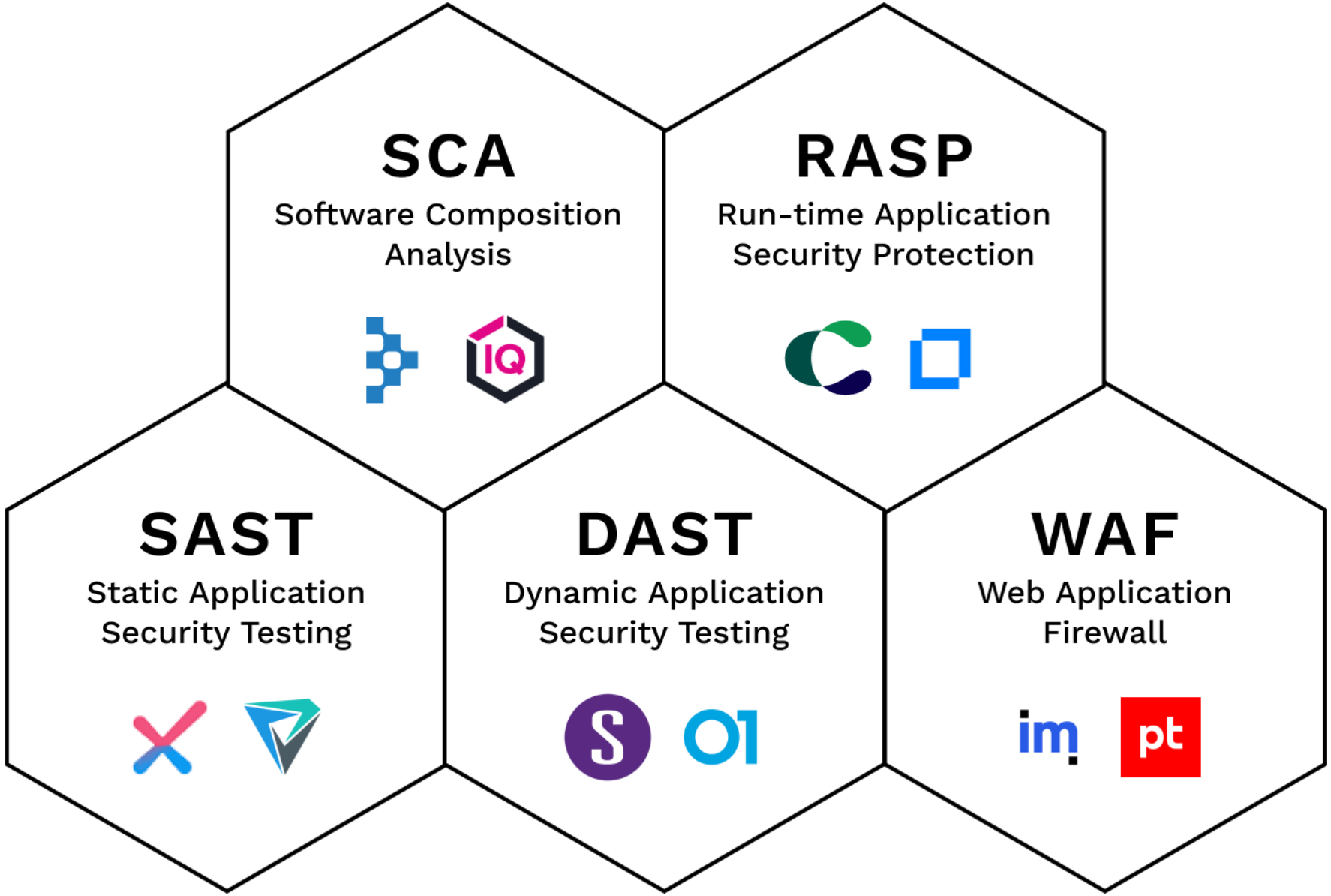
Что такое Shift-Left Security?

Shift-Left Security — внедрение проверок и практик безопасности в процессе SDLC так рано и так часто, как это возможно.

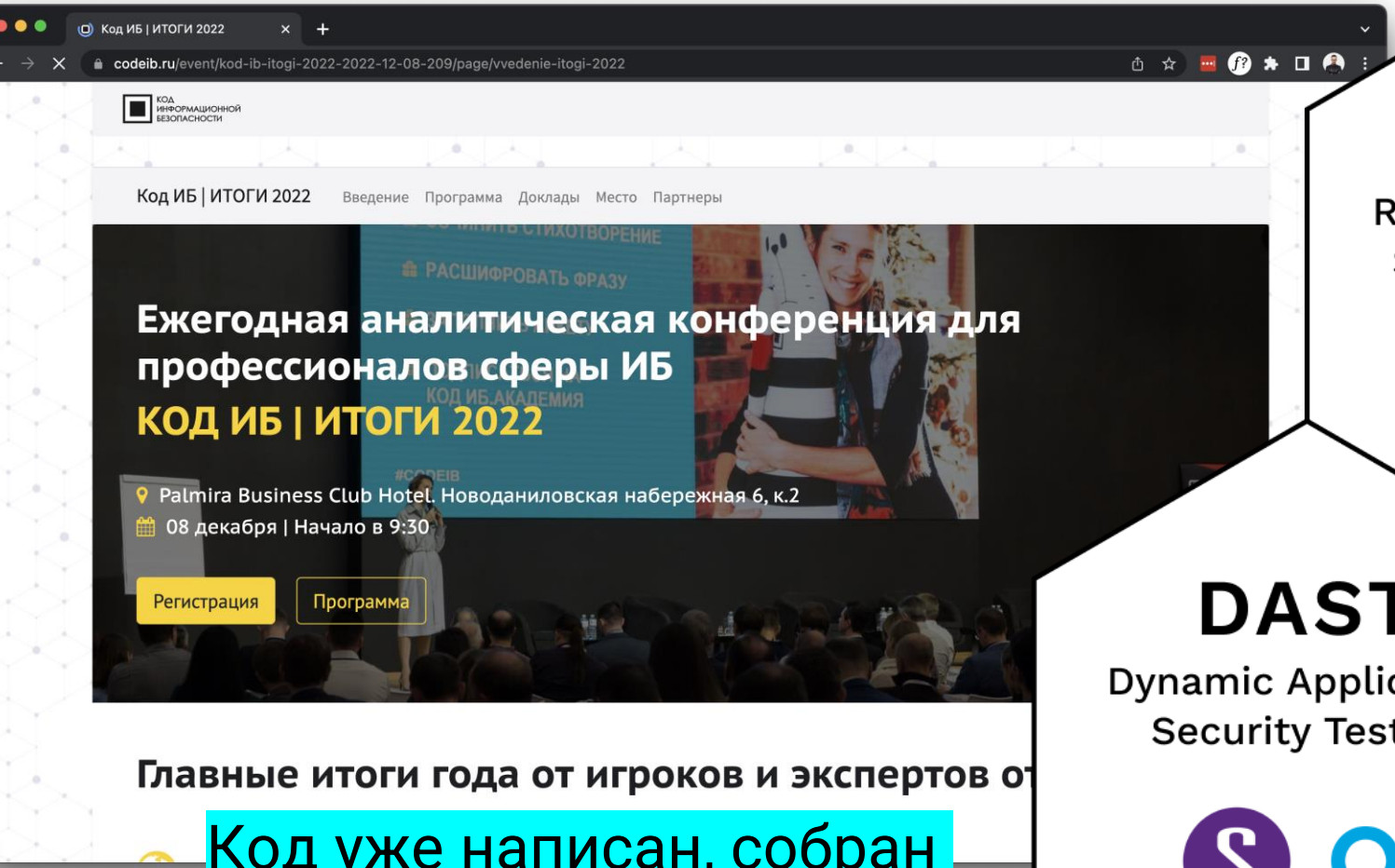
Устранение уязвимостей, выявленных как можно раньше в процессе разработки, значительно проще и обходится значительно дешевле



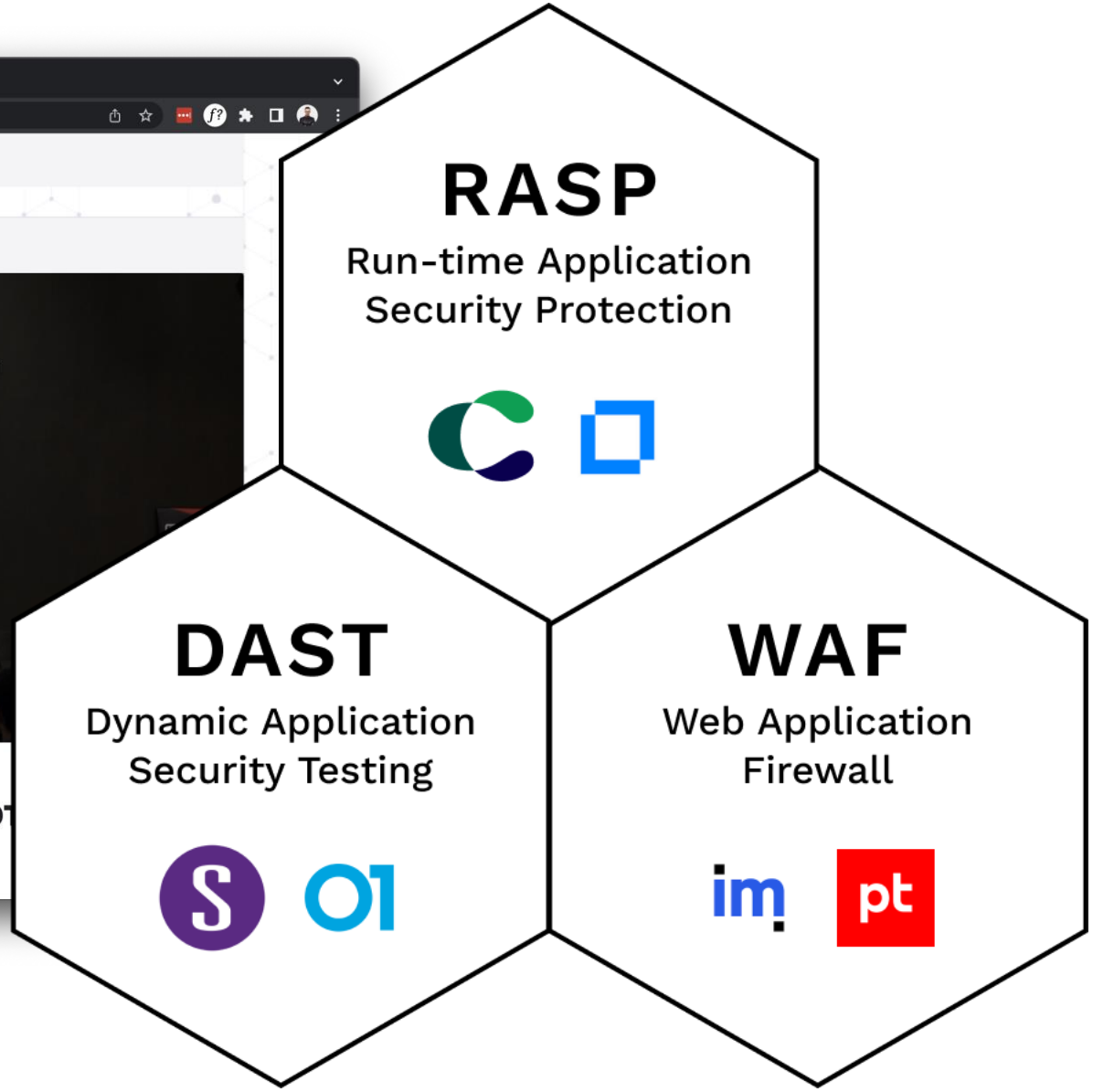
Какие инструменты делают продукт безопасным?

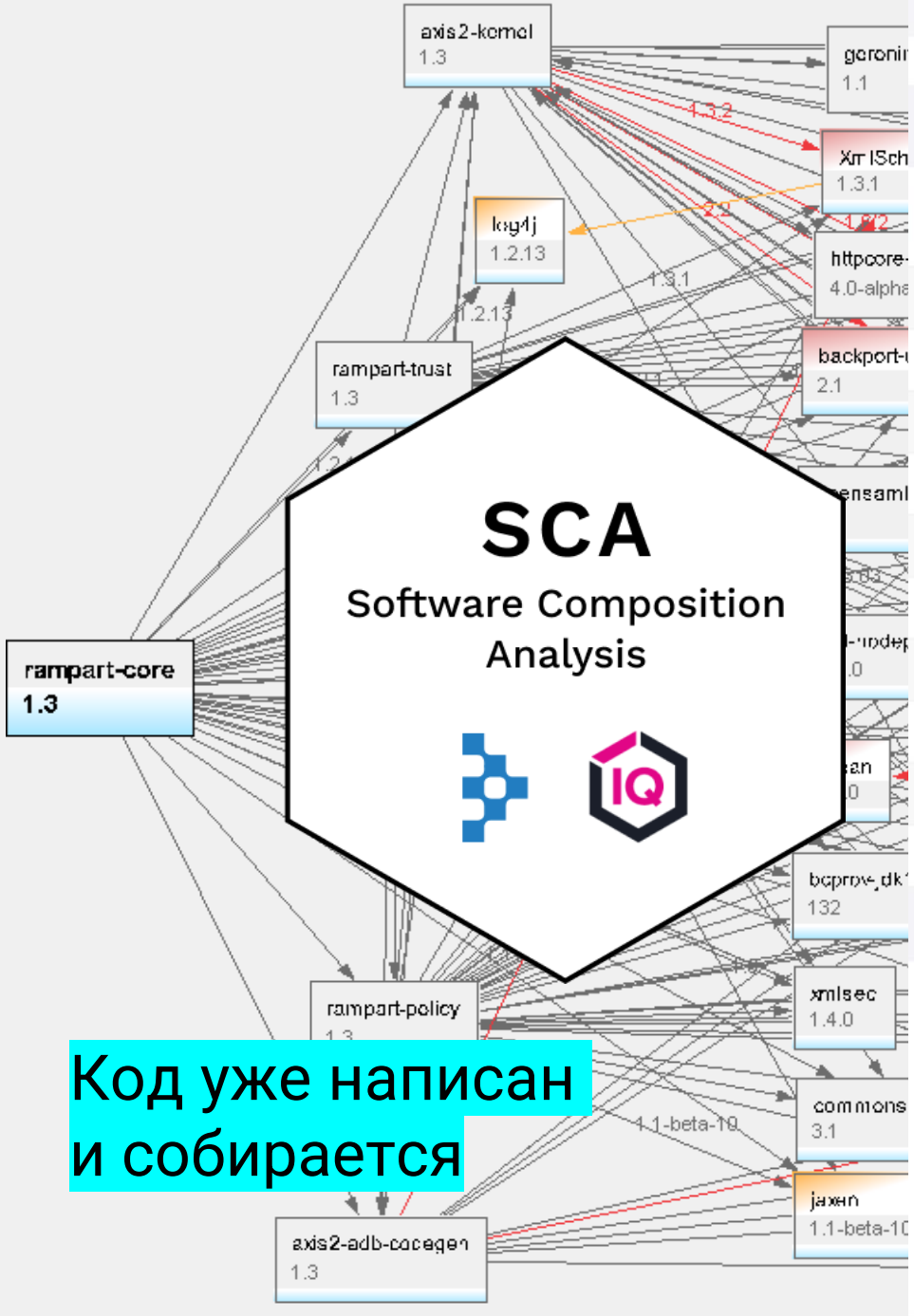


Какие инструменты делают продукт безопасным?



Код уже написан, собран и эксплуатируется





Код уже написан
и собирается

Dashboard › Antiphish

Build History trend

Filter builds...

#649	28 Sep 2022, 15:03
#648	26 Sep 2022, 11:59
#647	26 Sep 2022, 11:41
#646	23 Sep 2022, 17:28
#645	23 Sep 2022, 16:38
#644	23 Sep 2022, 10:33
#643	22 Sep 2022, 18:08
#642	22 Sep 2022, 17:23
#641	22 Sep 2022, 15:36
#640	20 Sep 2022, 17:47

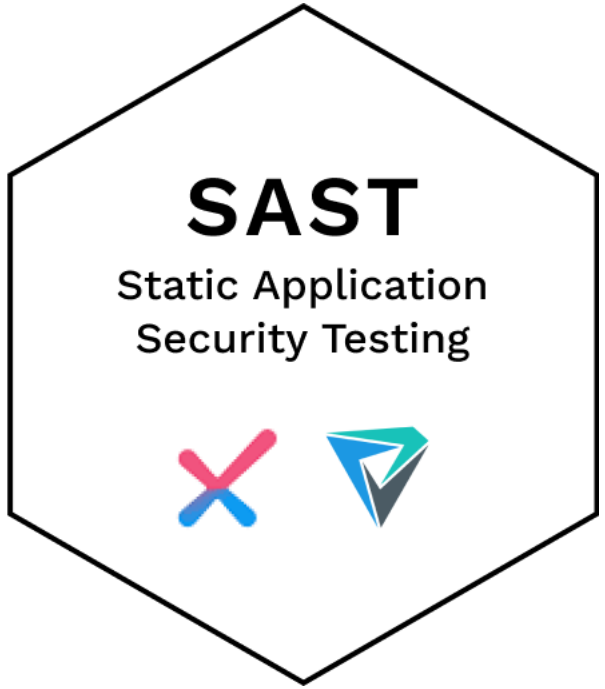
Atom feed for all Atom feed for failures

Stage View

	Checkout
Average stage times: (Average full run time: ~4min 46s)	52s
#649 Sep 28 15:03 — No Changes	21s
#648 Sep 26 11:59 — No Changes	59s
#647 Sep 26 11:41 — 3 commits	46s
#646 Sep 23 17:28 — 1 commit	54s
#645 Sep 23 16:38 — 4 commits	47s
#644 Sep 23 — 2	46s

Какие инструменты делают продукт безопасным?

Код уже написан

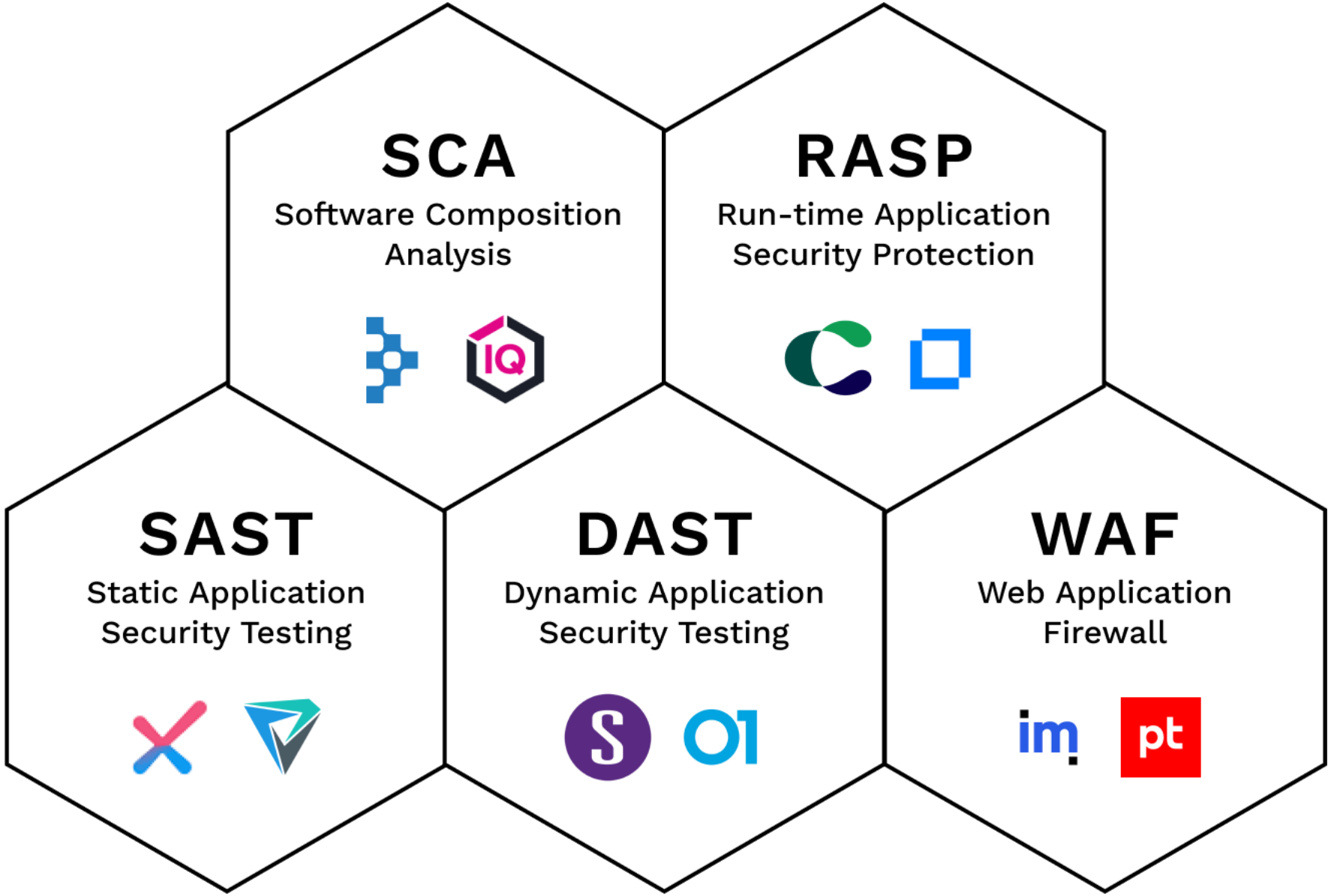


Что такое Shift-Left Security?

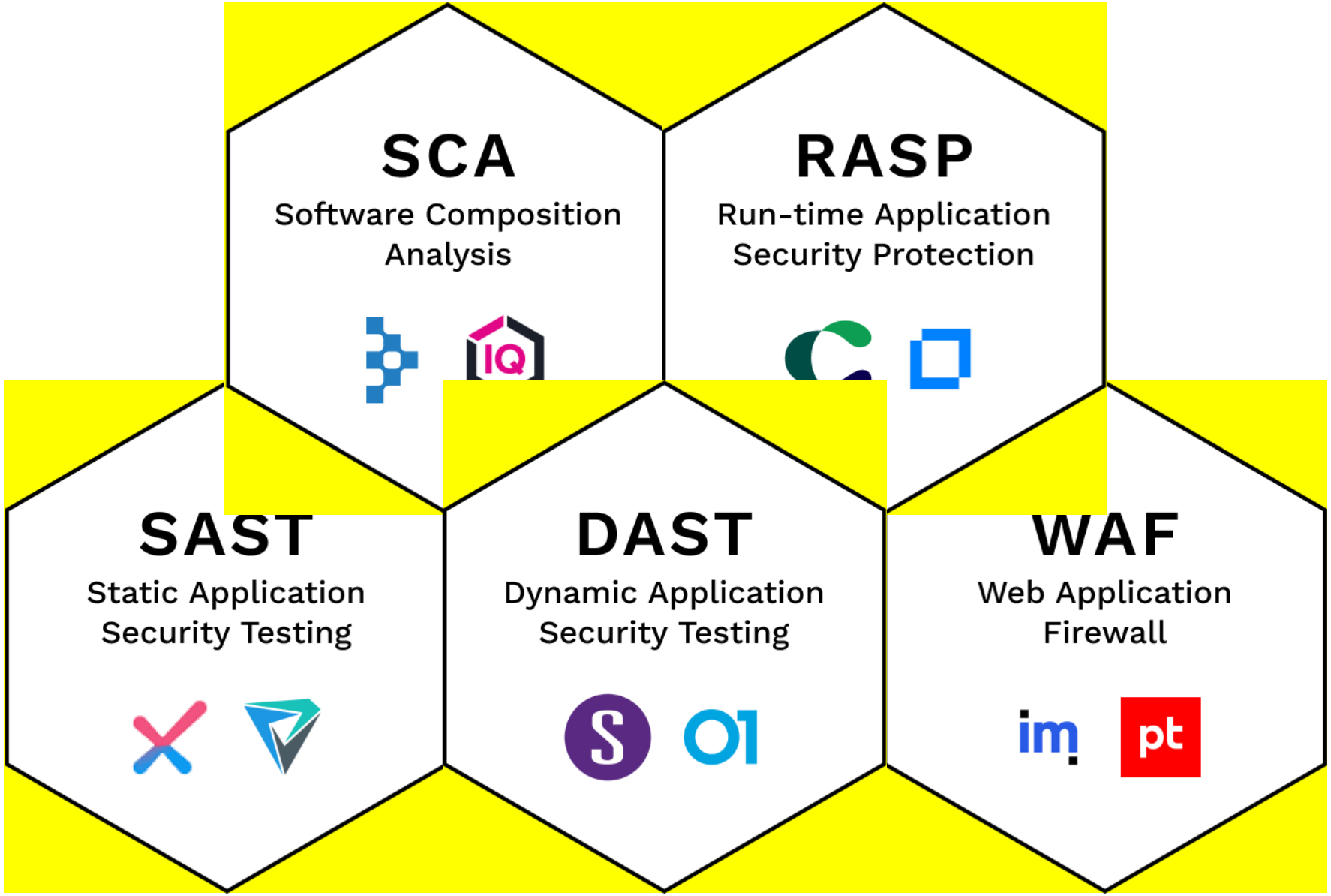
Планирование → Проектирование и дизайн → Реализация → Тестирование → Эксплуатация

Относительная стоимость устранения дефектов ПО на разных этапах разработки

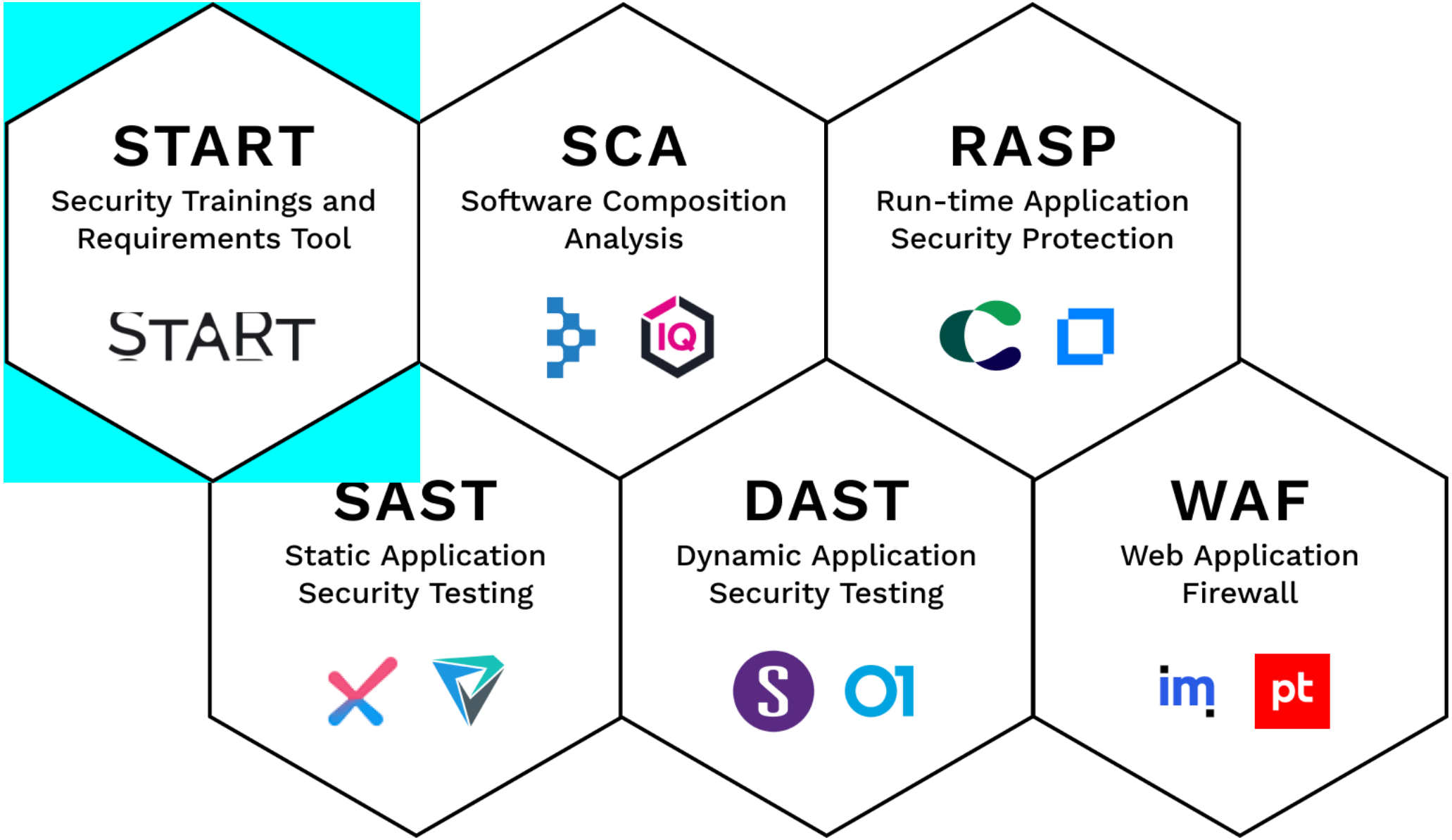
Какие инструменты делают продукт безопасным?



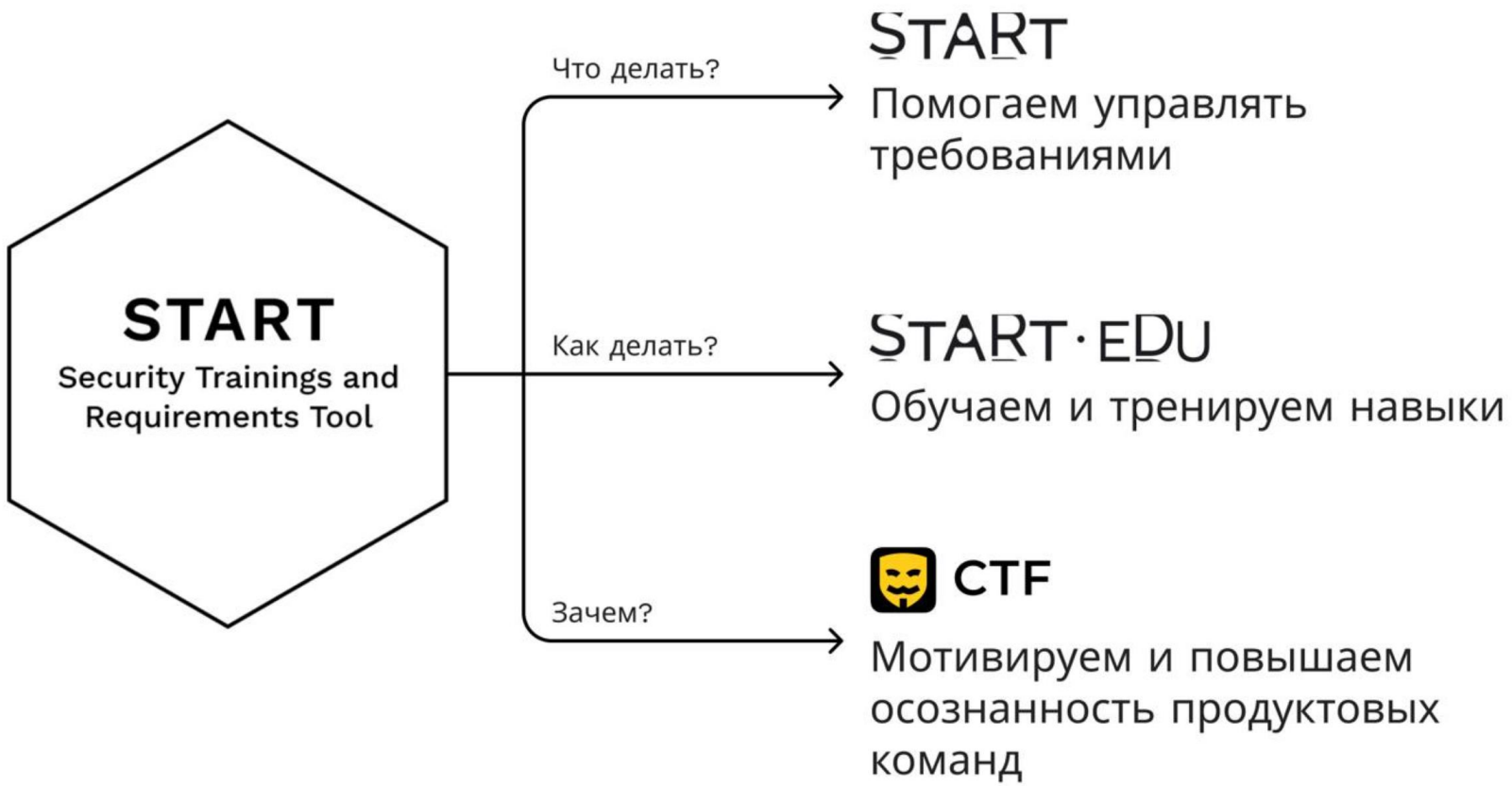
Инструменты не делают продукт безопасным



Люди делают продукт безопасным



Как подружиться с командам разработки и помочь им сделать безопасный продукт?



А разве и так не понятно, что делать?

При использовании сети "Интернет" для осуществления переводов денежных средств оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры обеспечивают применение организационных мер защиты информации и (или) использование технических средств защиты информации, пред отвращения несанкционирован емой информации путем остей программного обе

При наличии техни ператор по переводу денежны платежный агент (субагент), операто раструктуры обеспечивают выполнение предварительной проверки на отсутствие вредоносного кода программного обеспечения, устанавливаемого или изменяемого на средствах вычислительной техники, включая банкоматы и платежные терминалы

Сторонние open source-библиотеки, используемые для разработки, должны быть описаны в документации либо sbom (Software Bill of Materials) файле.

Использование компонентов с известными уязвимостями должно быть исключено.

Что не так с требованиями?

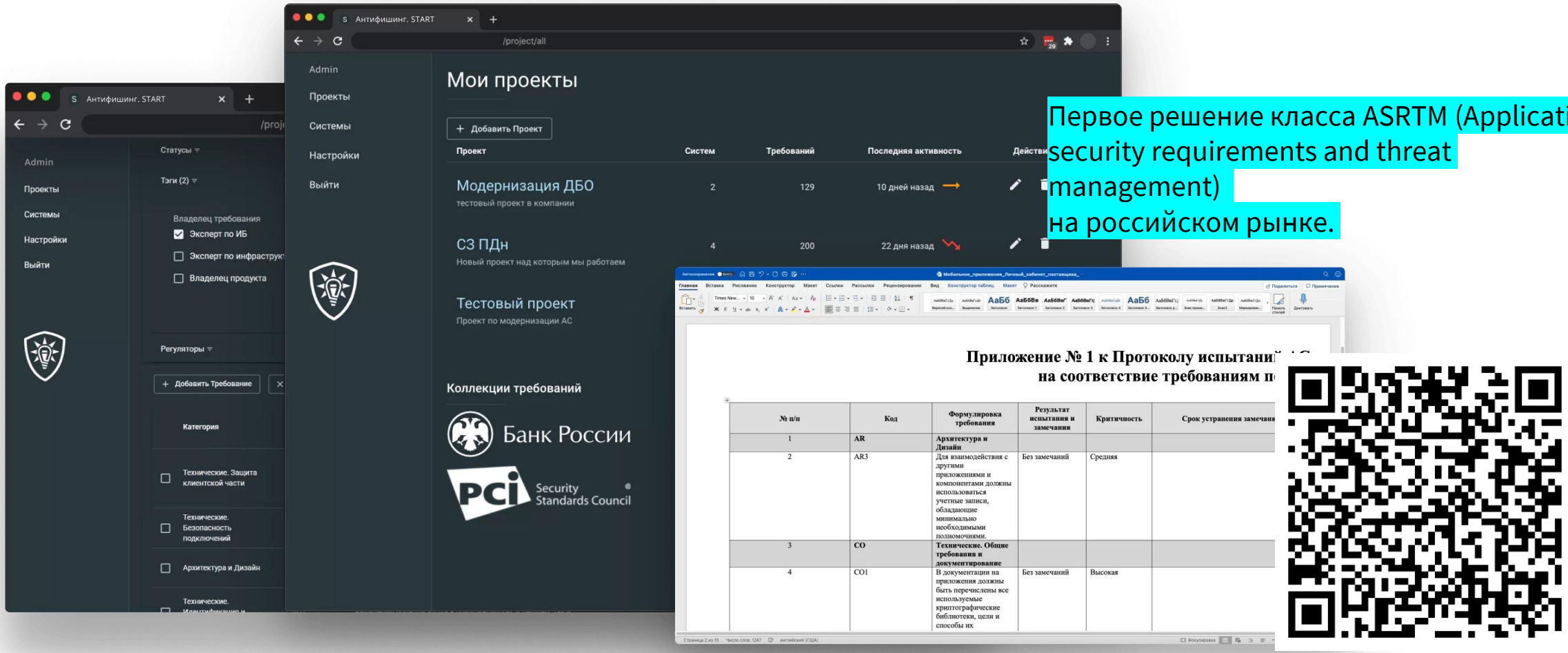
В случае принятия решения о необходимости использования одноразового кода подтверждения в целях аутентификации клиента при осуществлении переводов денежных средств с использованием системы Интернет-банкинга, а также при подтверждении клиентом права доступа к системе Интернет-банкинга, оператор по переводу денежных средств формирует и доводит до клиента информацию, необходимую для генерации одноразового кода подтверждения, ил дения, который:

•действителен на п риода времени, установленного опе ных средств;
•используется для п ва доступа к системе Интернет-банкинга оряжения (нескольких распоряжений) о р реводах) денежных средств или распоряжения ереводах денежных средств в определенную да лении определенных распоряжением (до
•однозначно соответствует сеансу использования системы Интернет-банкинга или распоряжению (распоряжениям, договору), подтверждаемому (подтверждаемым) клиентом с использованием системы Интернет-банкинга;
•доводится до клиента по альтернативному системе Интернет-банкинга каналу связи, или входит в набор возможных одноразовых кодов подтверждения, который доводится до клиента оператором по переводу денежных средств на материальном носителе, или создается клиентом с использованием технического средства, предназначенного для генерации одноразовых кодов подтверждения

Финансовые операции должны подтверждаться с использованием одноразовых паролей с настраиваемым временем жизни.

Пароли должны отправляться на номера Клиентов через SMS

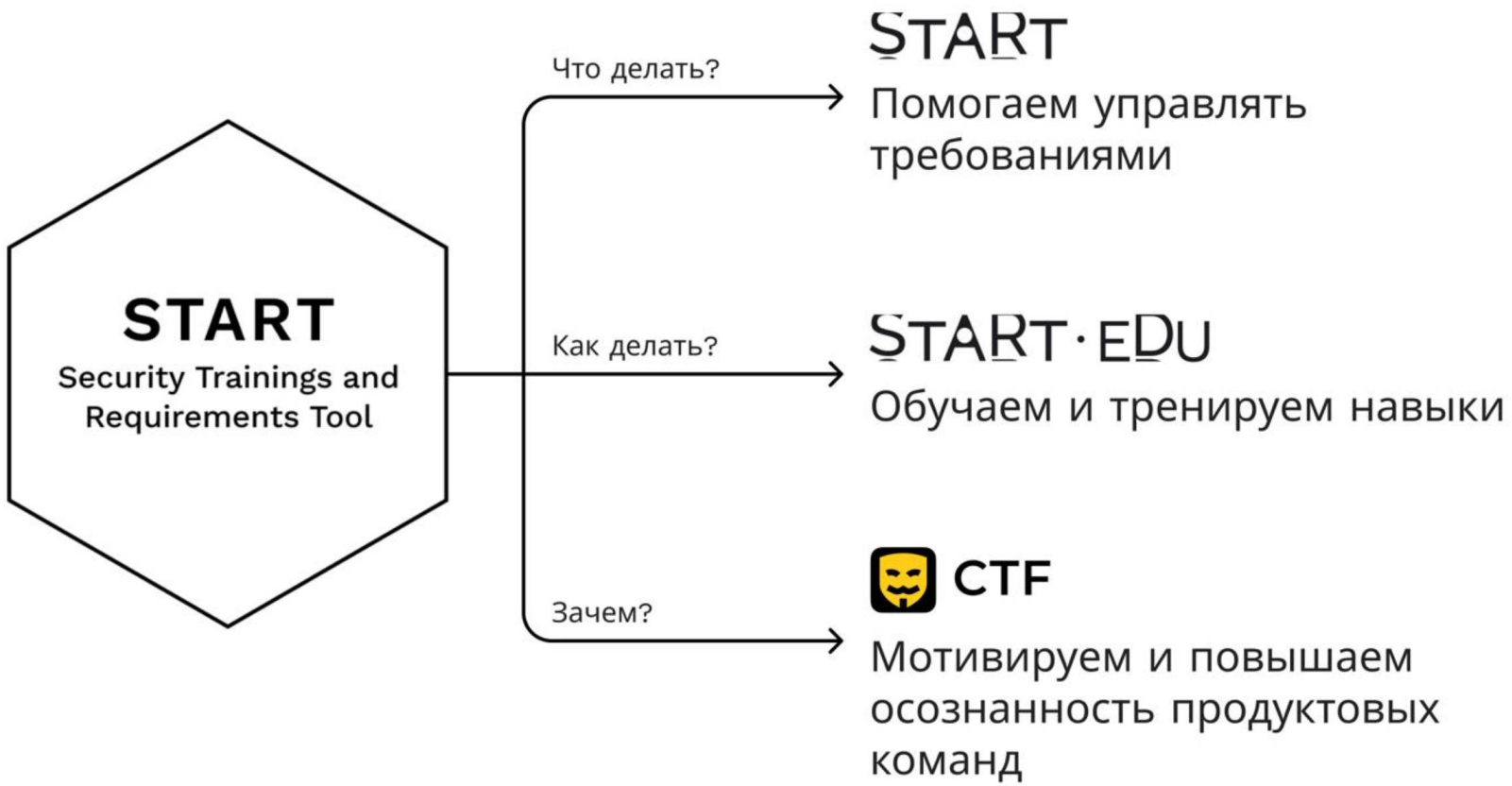
Антифишинг. START для продуктовых команд



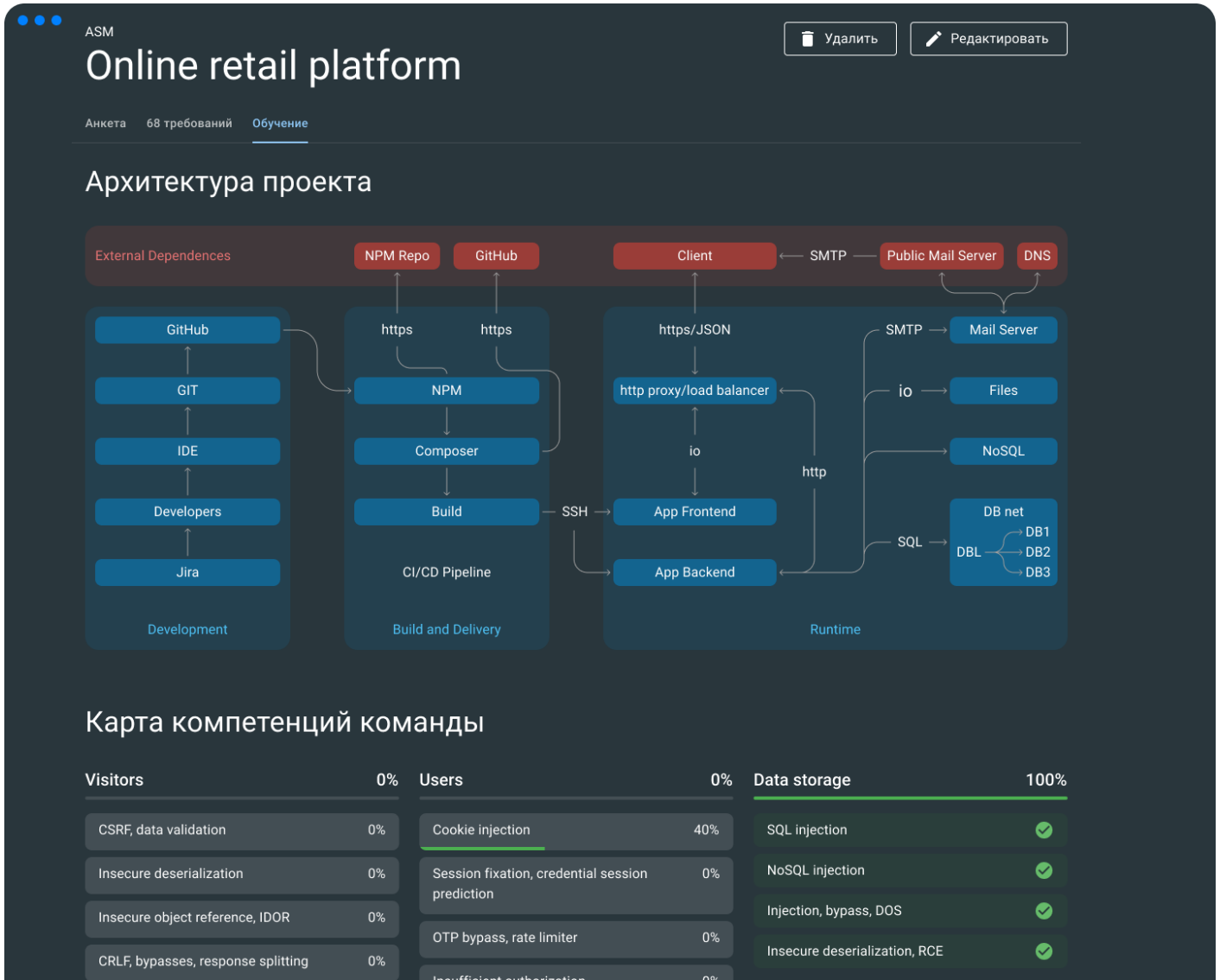
Первое решение класса ASRTM (Application security requirements and threat management) на российском рынке.

Система для управления требованиями и знаниями по безопасности приложений, а также для обучения разработчиков ПО и продуктовых команд вопросам безопасной разработки.

Как подружиться с командам разработки и помочь им сделать безопасный продукт?



Антифишинг. START. EDU — интерактивный модуль обучения для продуктовых команд



Jira

Строит карту проекта

Назначает только актуальные обучающие модули

Доставляет знания и навыки прямо в Jira

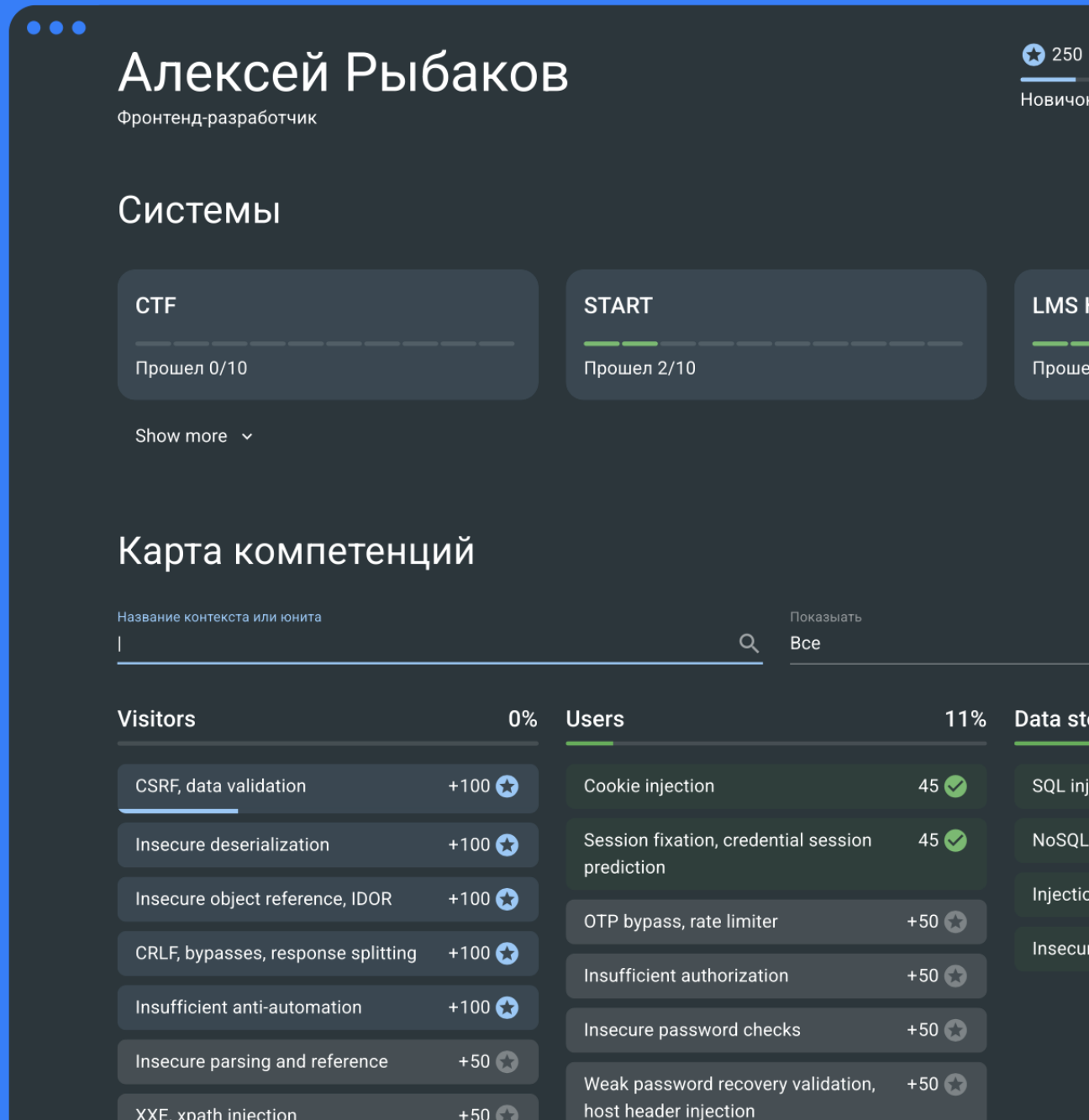
START.EDU

Модуль интерактивного обучения команд актуальным вопросам безопасной разработки в рамках продукта Антифишинг.START.

Платформа за 15 минут выявит навыки разработчиков через тестирование и автоматически составит матрицу их компетенций.

Каждому разработчику подбирается обучающий курс, согласно навыкам и текущим проектам, в которых он задействован.

START

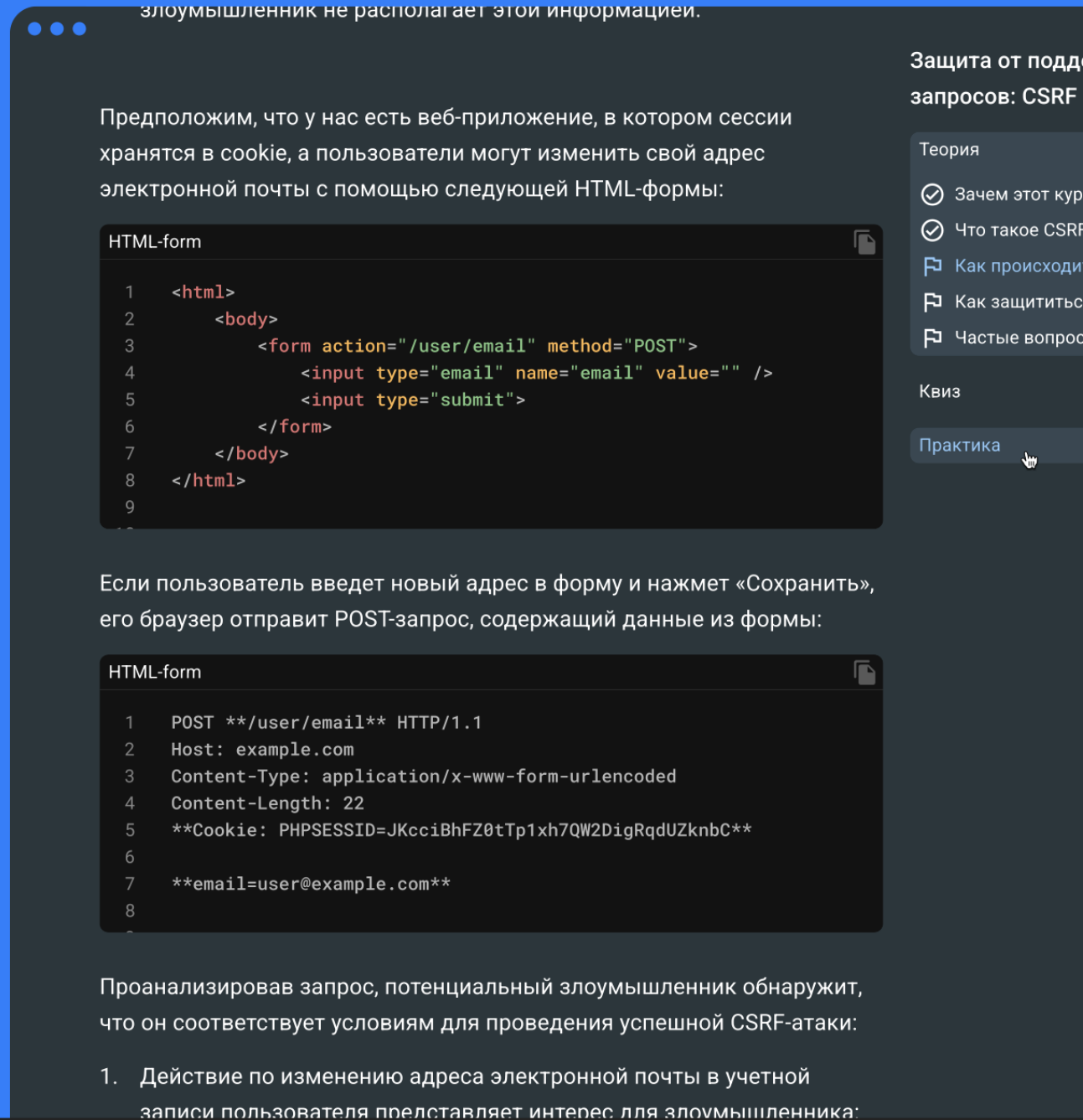


START.EDU

Каждый курс состоит из юнитов с актуальной теорией, обязательными примерами из реальной среды и проверочными заданиями, которые основаны на кейсах уязвимых приложений и помогают закрепить и проверить полученные знания.

Интеграция с JIRA синхронизирует обучение с другими рабочими процессами.

START



Шаг 4. Теория и примеры кода

Сотрудники получают доступ к учебным модулям гибридной структуры

Предположим, что у нас есть вео-приложение, в кото
cookie, а пользователи могут изменить свой адрес эл
помощью следующей HTML-формы:

HTML-form

```
<html>
    <body>
        <form action="/user/email" method="POS
            <input type="email" name="email" v
            <input type="submit">
        </form>
    </body>
</html>
```

Если пользователь введет новый адрес в форму и на
браузер отправит POST-запрос, содержащий данные

HTML-form

```
POST **/user/email** HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencode
Content-Length: 22
```

Java Python JavaScript PHP ASP.NET

SPRING FRAMEWORK GOOGLE WEB TOOLKIT

В данном фреймворке создание (`ResponseCookie`) и отправка (`ResponseEntity`) cookie происходит с помощью пакета `org.springframework.http`

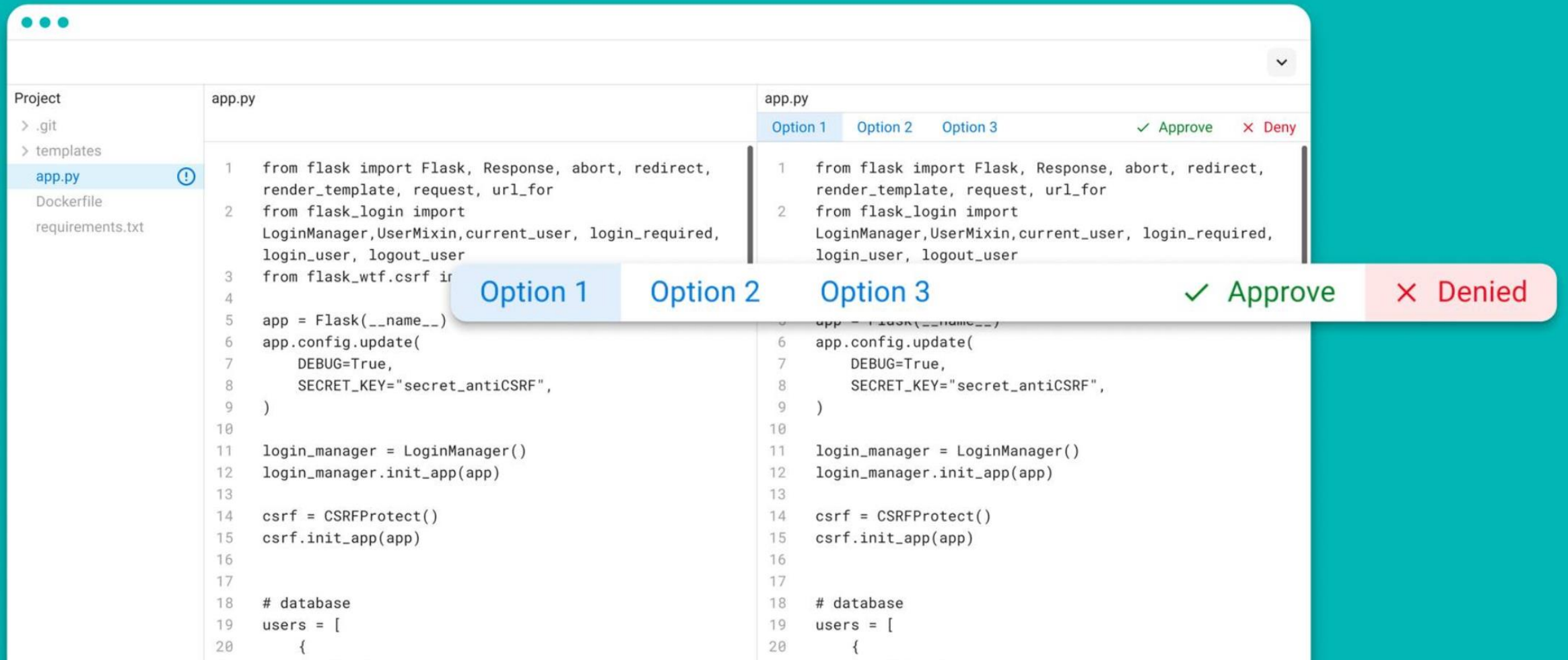
Начиная с версии Spring Security 4.x защита от CSRF включена по умолчанию. Соответствующий управляющий атрибут `_csrf` принадлежит объекту HttpServletRequest.

Обязательное требование CSRF-токена можно отключить (хотя делать это мы крайне не советуем) следующим образом:

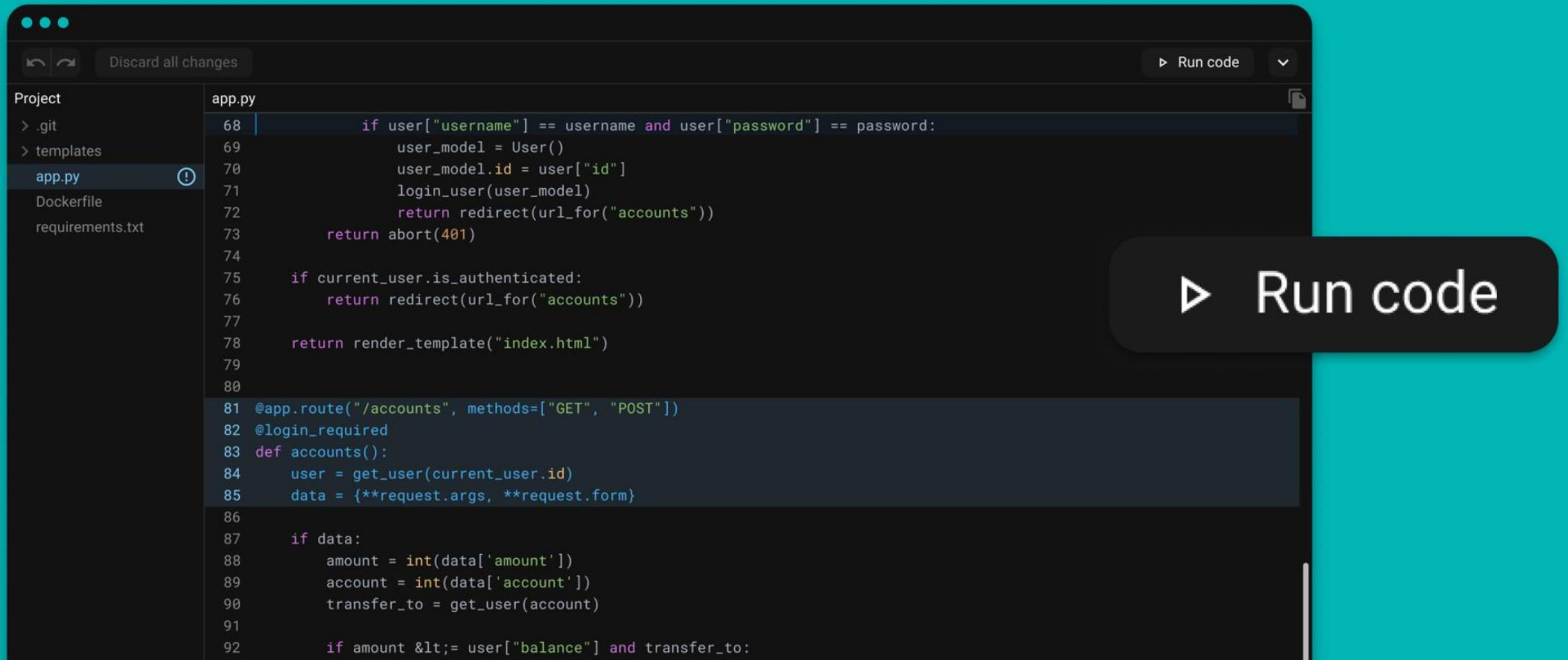
Java

```
@Override
protected void configure(HttpSecurity http) throws Exception {
    http.csrf().disable();
}
```

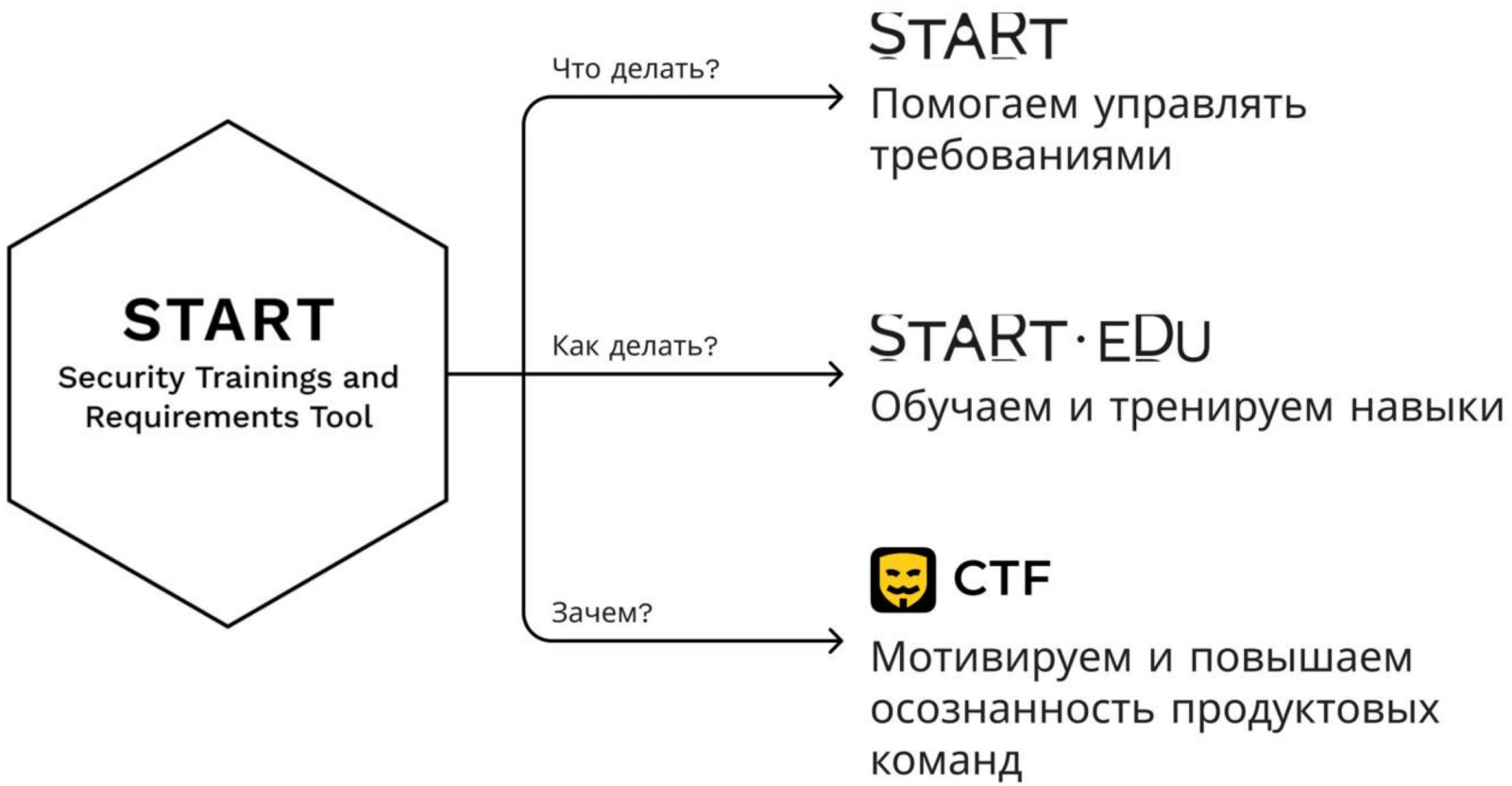
Шаг 6. Практика ревью кода



Шаг 7. Практика с написанием кода, Q2 2023

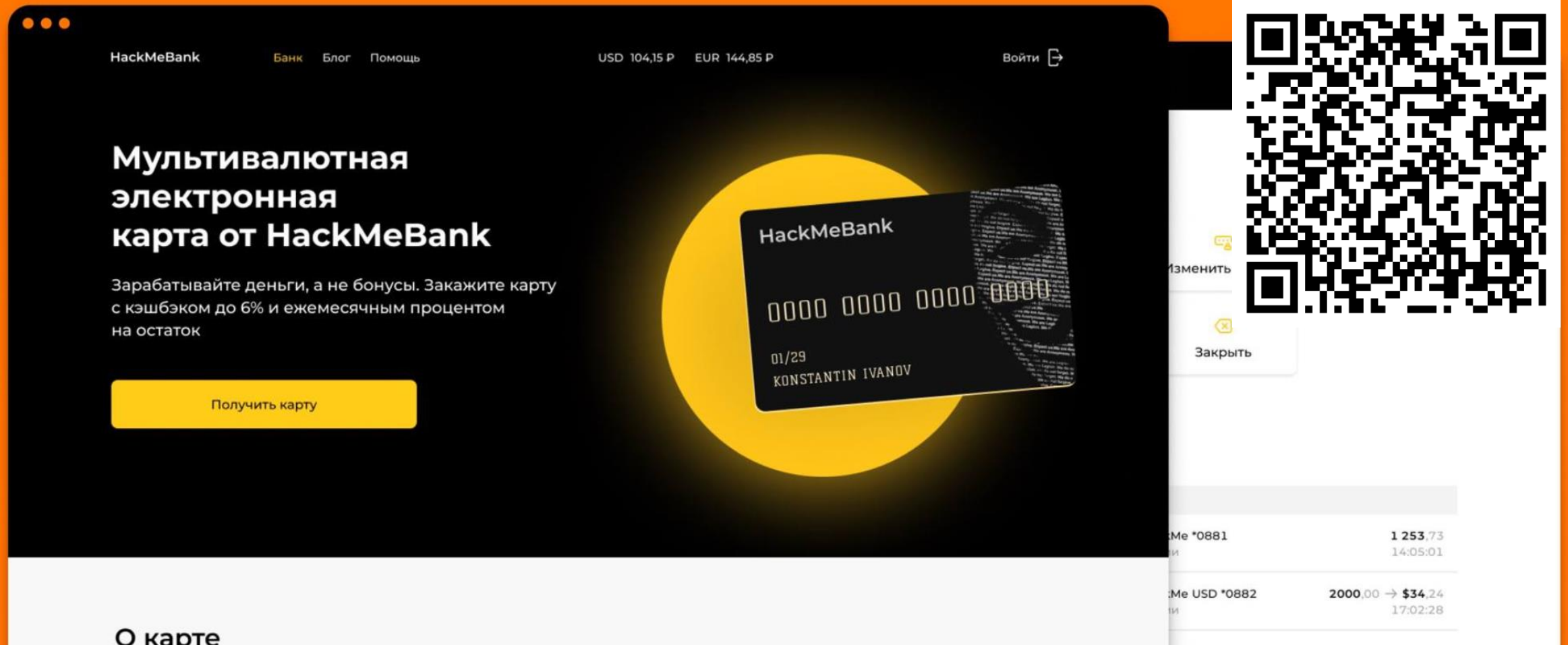


Как подружиться с командам разработки и помочь им сделать безопасный продукт?



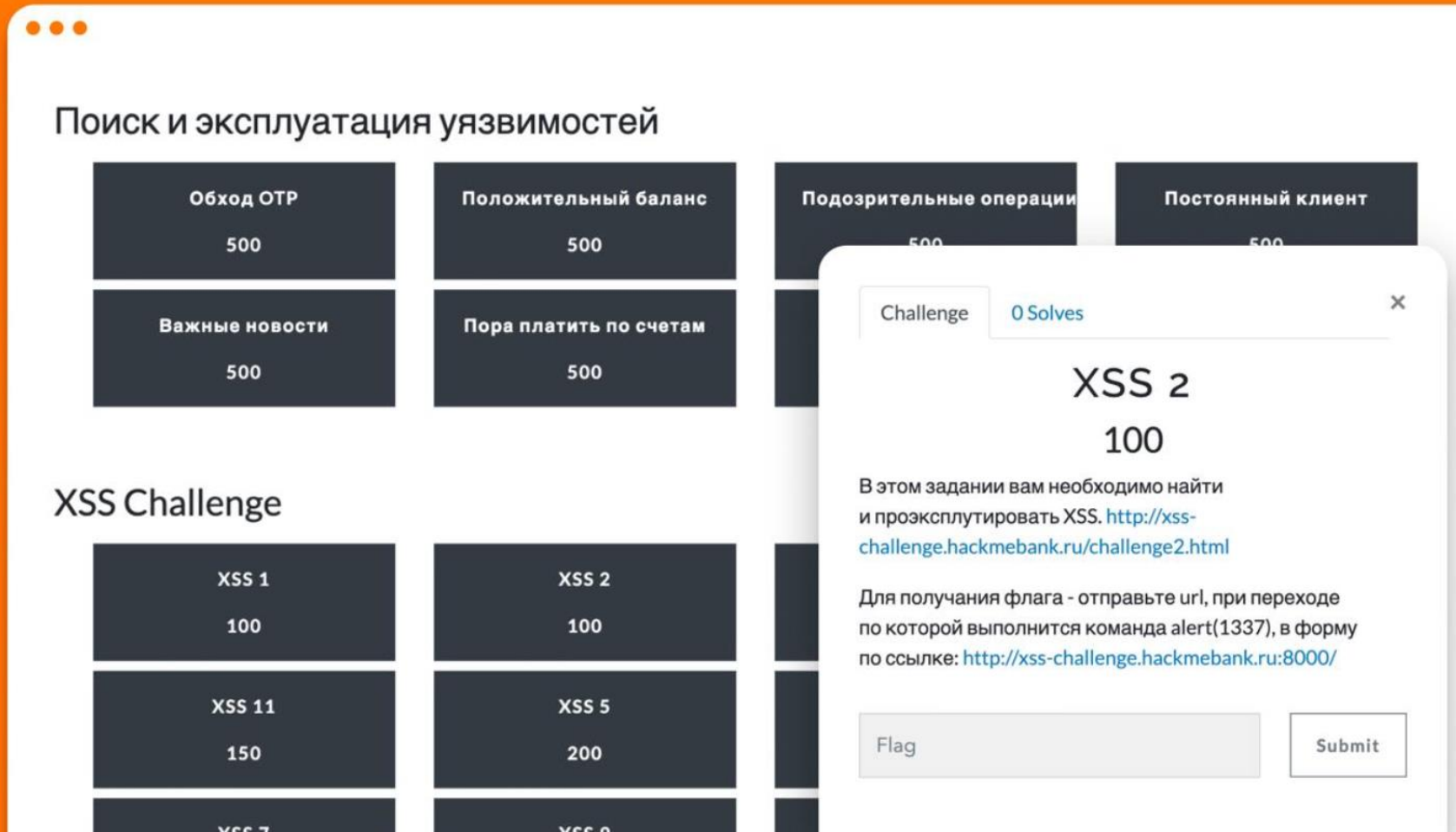
START.CTF

Тренажер по практической безопасности в формате действующего интернет-банка



START.CTF

Тренажер по практической безопасности в формате действующего интернет-банка



4 недели

длится соревнование

Вопросы про безопасность — продвинутый уровень

— Аутентификация при межсесрвисном взаимодействие работает очень медленно, лучше без нее?

— Это точно не работает из-за межсетевого экрана, давайте сделаем досутуп any-any для проверки?

— Quality Gate по безопасности вернулся со статусом fail, но мы точно ничего важного не меняли, пойдем в прод без него?

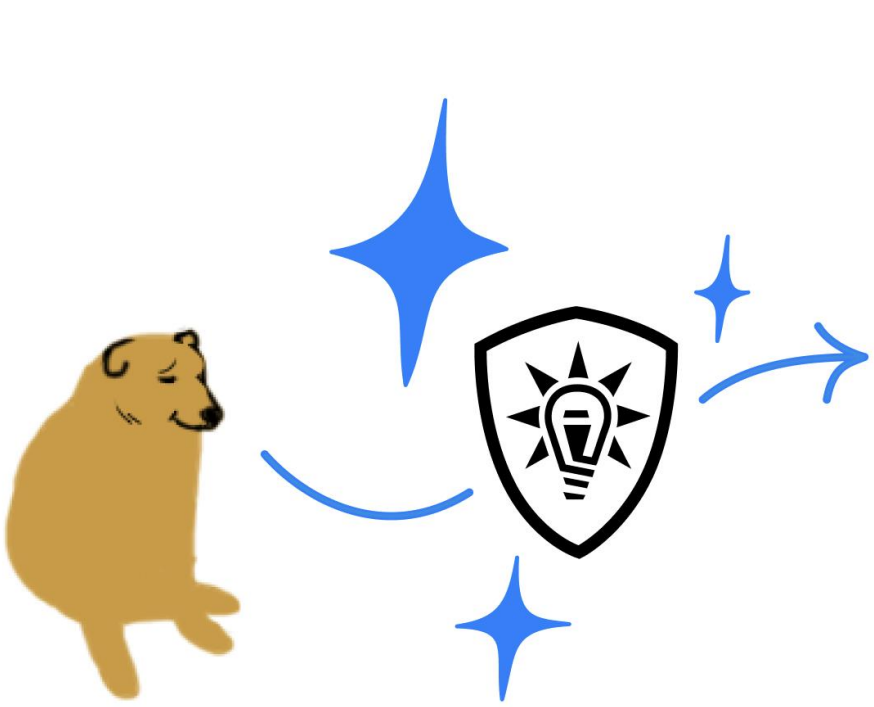
Ответы сотрудников на такие вопросы – и есть культура безопасности компании

Ответы крутых продуктовых команд

1. Разработчик нашел уязвимость в бизнес-логике, которая раскрывает данные по клиентам и может привести к социальной инженерии.

3. Был баг с файрволом на одном из кластеров и программист заменил открытый 22 порт когда что-то искал в shodan. Сообщил, потом мы уже обнаружили баг в proxmox

2. SRE собрали
партнеру, парт
стороны перед
решил попракт
И во время ана
обратный прок
обращался к lo
Оказалось, что
видимо кто-то
2007 году встро



одном из
етили
компания
их
е только

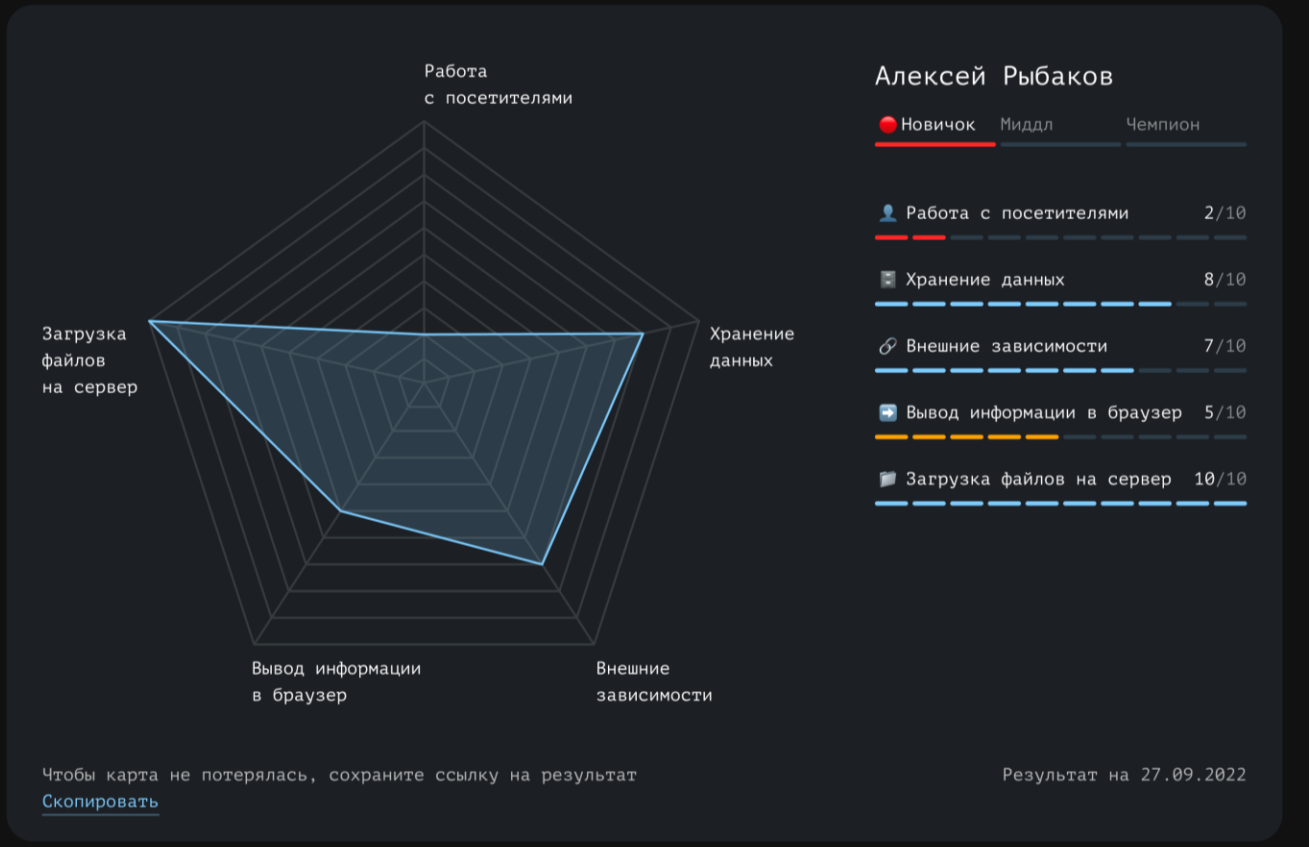
Тест для продуктовых команд

Security Champion

Узнайте, кто из ваших коллег — настоящий Security Champion.

Как выглядит результат

После прохождения составляем карту компетенций, на которой показываем уровень навыков и разработчика в целом



Узнайте, кто из ваших коллег — настоящий Security Champion.

Оцените навыки и получите карту компетенций для каждого члена команды за 15 минут.

edu.antph.net

Продукты «Антифишинга» уже используют

Ростелеком

X5 Group

М.ВидеоЭльдорадо

QIWI

НСПК
НАЦИОНАЛЬНАЯ СИСТЕМА ПЛАТЕЖНЫХ КАРТ

ГАЗПРОМБАНК

Газпром нефть

ИНТЕР РАОЕЭС

AirBridgeCargo

START

CTF

Как вести безопасную разработку и создавать защищённые продукты

Используйте наши рекомендации, чтобы ваши процессы и продукты соответствовали лучшим практикам безопасной разработки

antiphish.ru/products/start

devsecops@antiphish.ru

Шаги по разработке защищенного продукта

1
Создайте собственный каталог требований

2
Используйте модель обеспечения безопасности ПО OWASP

3
Пишите безопасный код

4
Делайте качественный код-ревью

5
Используйте CI-системы правильно

6
Применяйте статический анализатор

7
Проверяйте собственное тестовое окружение

9
Проводите ручное тестирование

10
Проводите внутренние пентесты

11
Повышайте квалификацию разработчиков

www.antiphish.ru
ask@antiphish.ru

Начните дружбу
с продуктовыми
командами