

АНТИФИШИНГ

Shift-Left Security: как подружить
безопасность и продуктивные команды

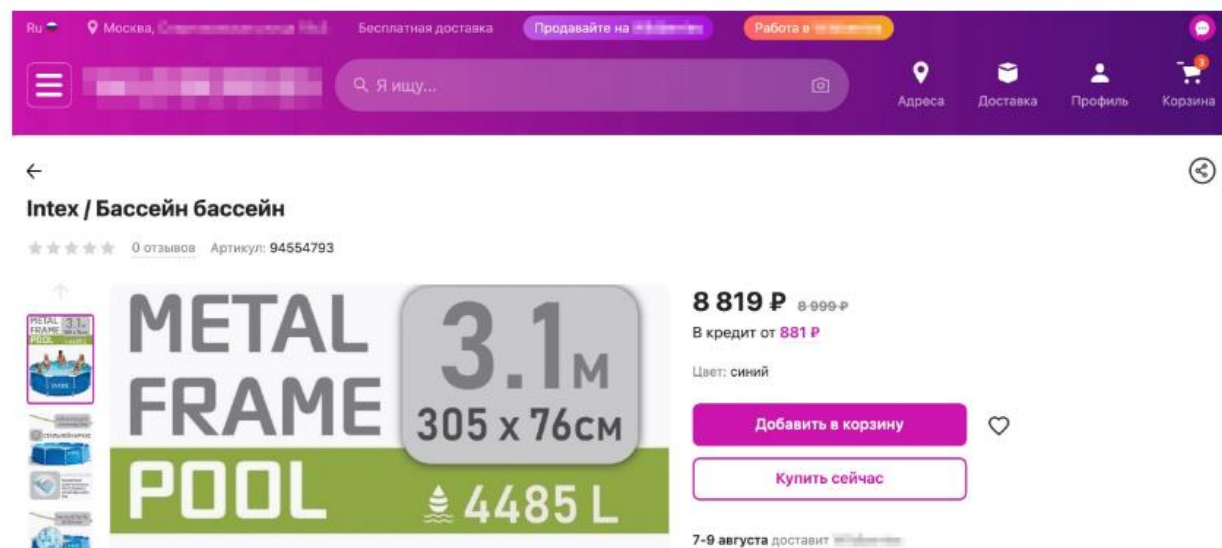
blog.antiphish.ru

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.



t.me/antph



Андрей Жаркевич
редактор



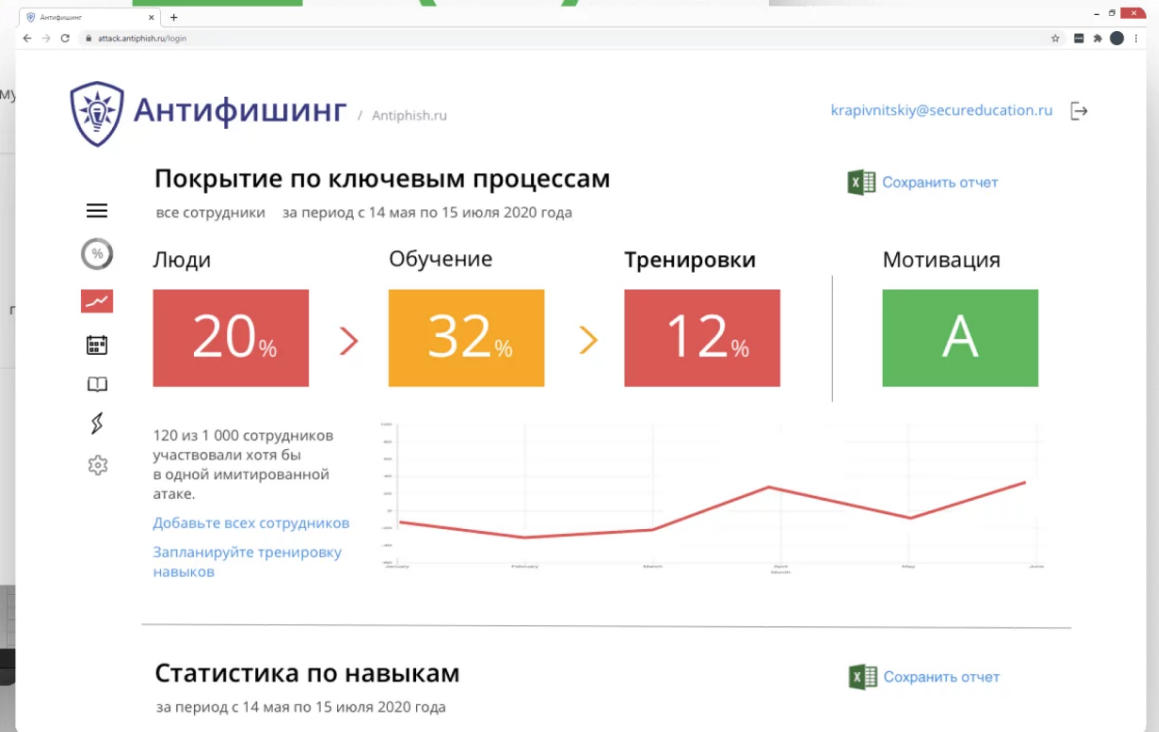
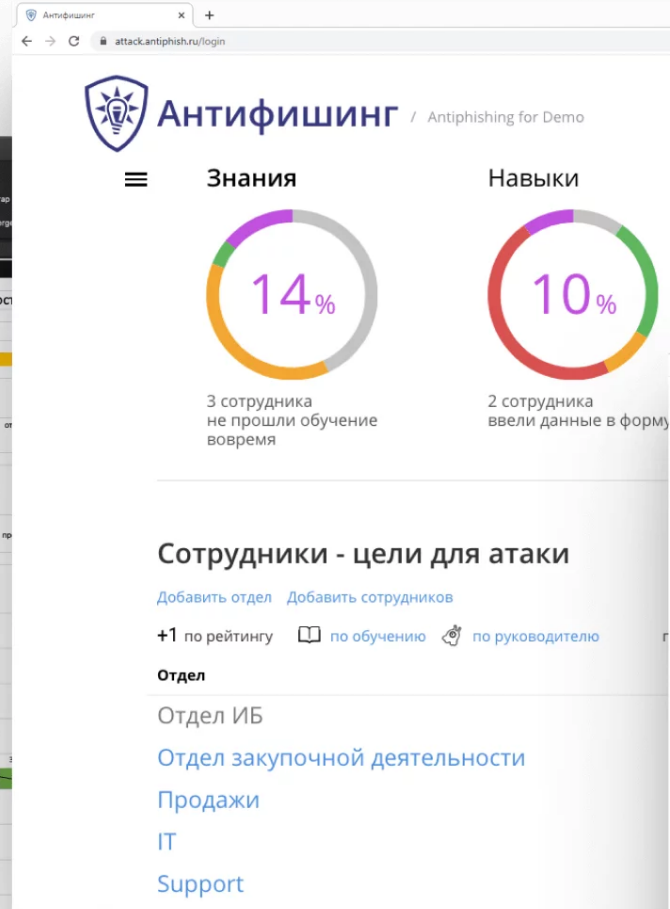
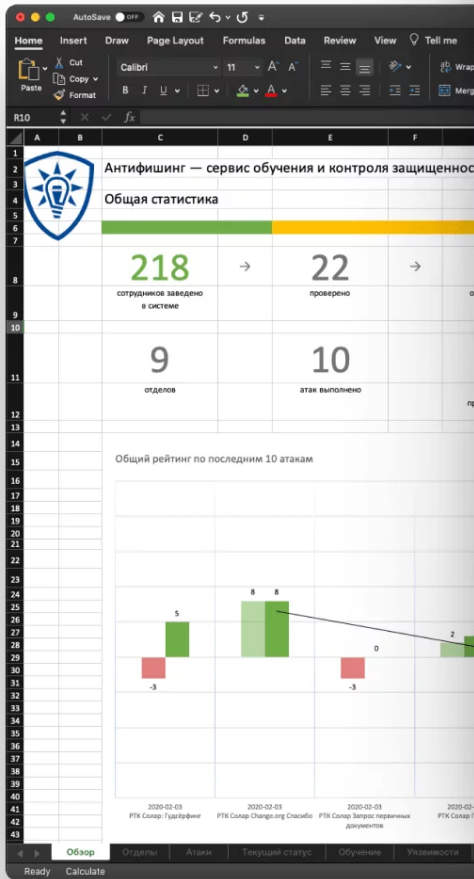
Артемий Богданов
технический директор



Сергей Волдохин
выпускающий редактор



A Антифишинг для всех сотрудников



Askona Блог

Клиент в фокусе: как «Аскона» и менила потребительский опыт

..... <

Новости 12.10.20

19:25
SpaceX отправит первого в истории космического туриста в полет вокруг Луны

Forbes

Миллиардеры

Читайте о людях, владевших и владеющих крупнейшими состояниями в России и мире

Информационная безопасность

26.01.2022, 00:47

Вирус взял подработкой

В доработанных модулях 1С нашли вредоносный код

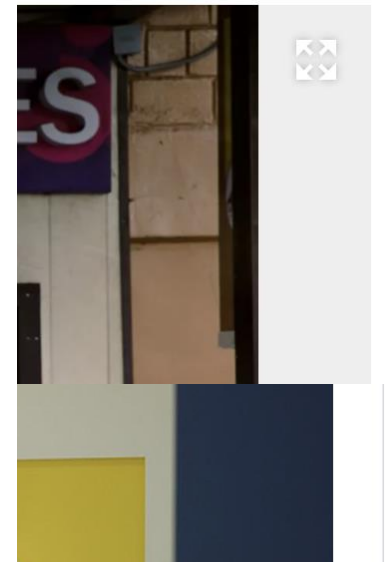
- 33К
- 4
- 2 мин.
-
-
-
-

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
ыстрым 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 основном загружали пакеты из основных общедоступных репозиториях NPM, PyPI и RubyGems, которые считались приоритетными.

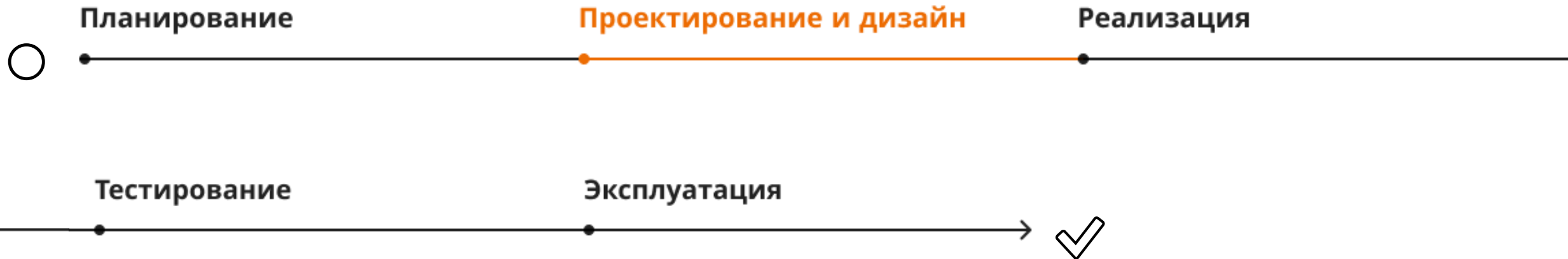
Присутствие похожих пакетов с такими же именами в репозиториях игнорировалось без отображения предупреждений и сбоя для администраторов. В PyPI на приоритет загрузки влиял номер версии (всегда была загружена самая последняя версия пакета). В NPM и RubyGems приоритет отдавался только от репозитория.



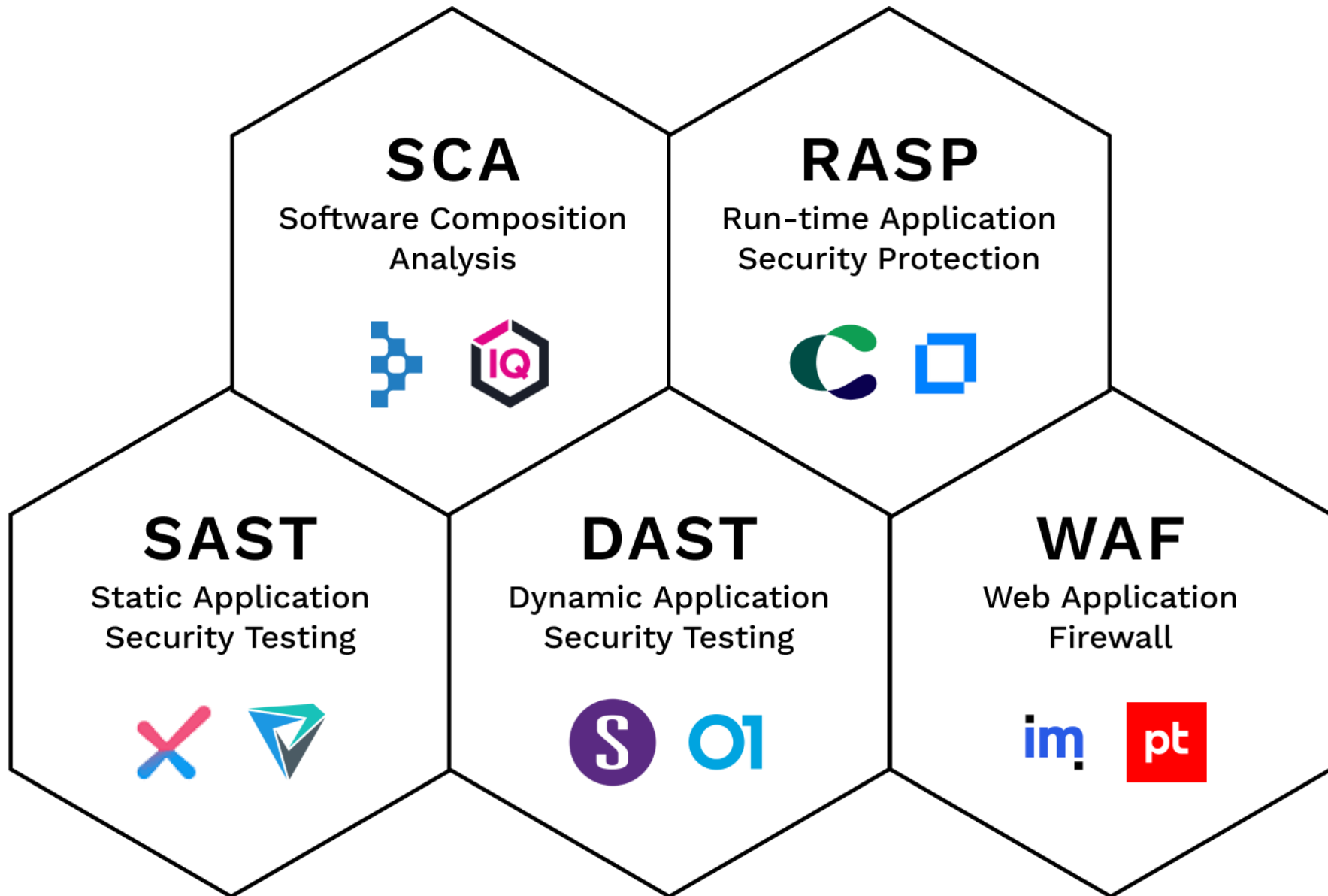
A Что такое Shift-Left Security?

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

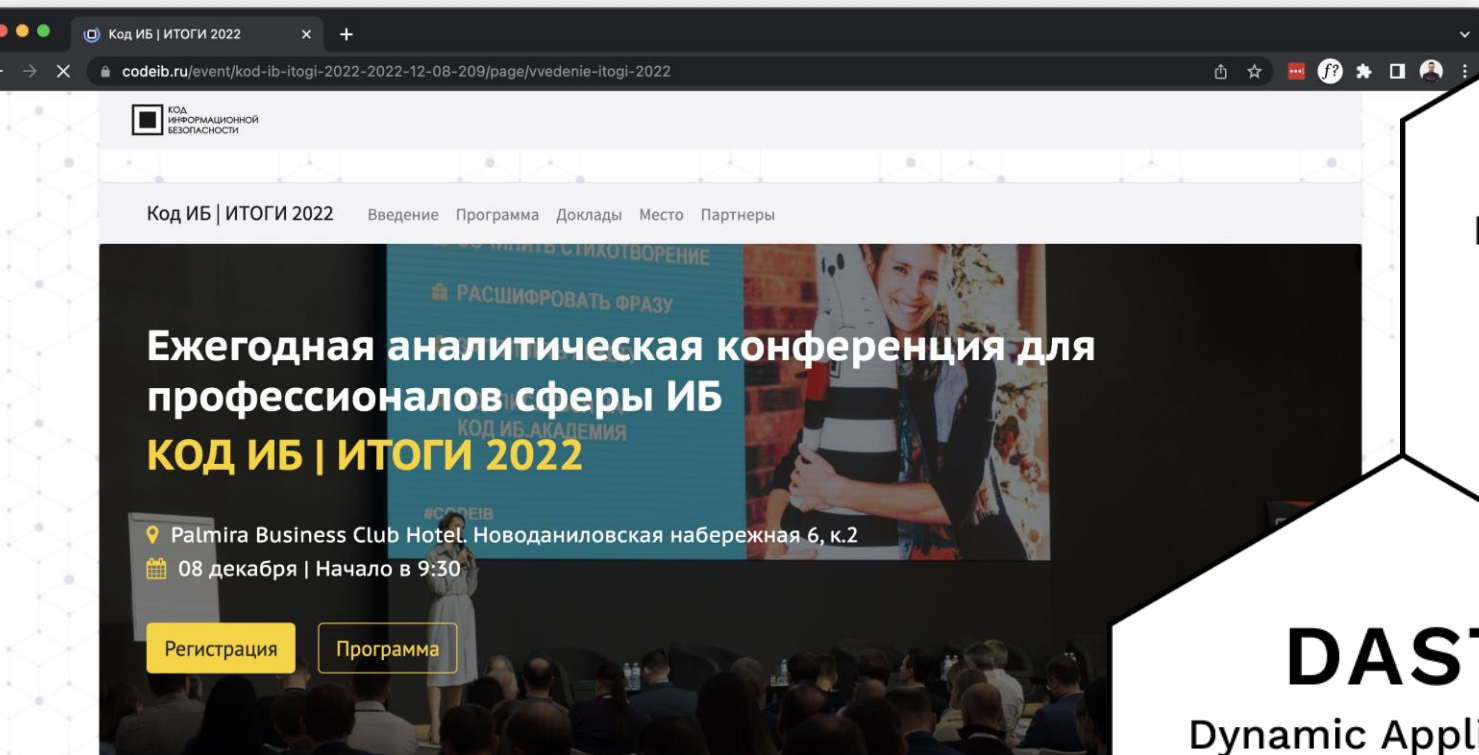
Устранение уязвимостей, выявленных как можно раньше в процессе разработки, значительно проще и обходится значительно дешевле



A Какие инструменты делают продукт безопасным?



A Какие инструменты делают продукт безопасным?



Главные итоги года от игроков и экспертов о

Код уже написан, собран и эксплуатируется

RASP
Run-time Application
Security Protection



DAST
Dynamic Application
Security Testing



WAF
Web Application
Firewall

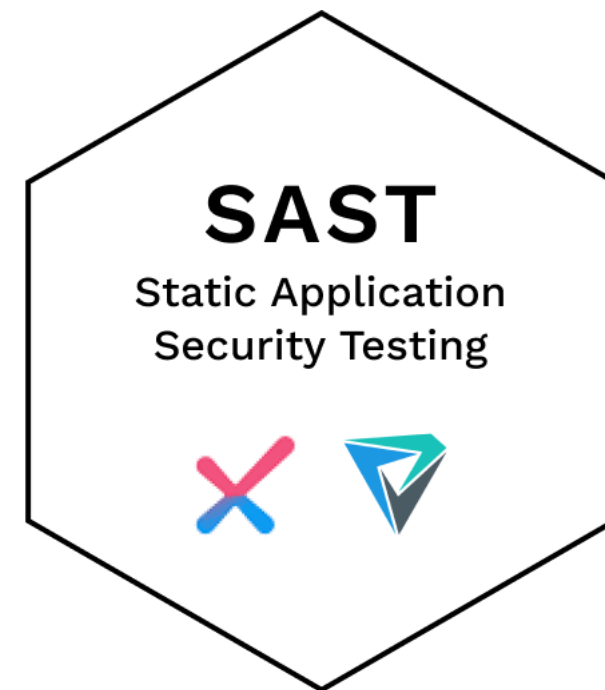
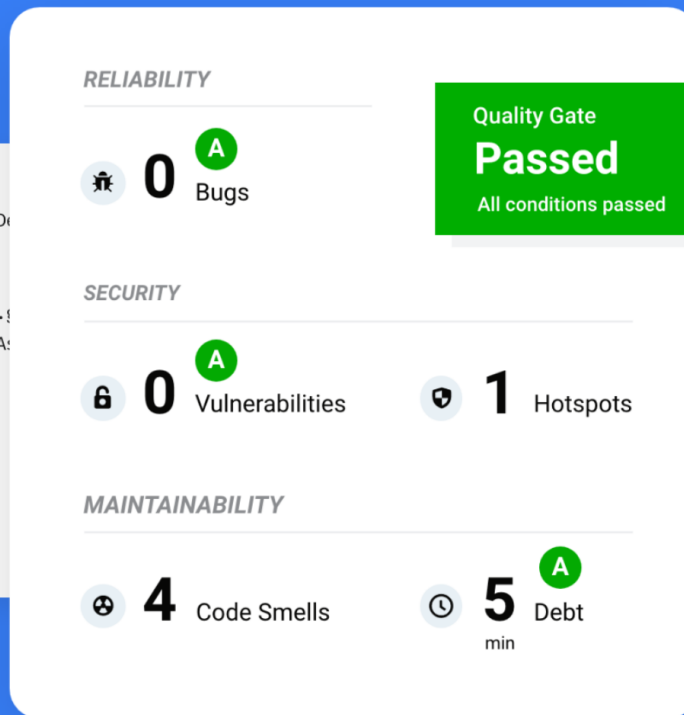


A Какие инструменты делают продукт безопасным?

```
246 if (Provider.class == roleTypeClass) {
247     Type providedType = ReflectionUtils.getLastTypeGenericArgument(dependencyDescriptor);
248     Class providedClass = ReflectionUtils.getTypeClass(providedType);
249
250     if (this.componentManager.hasComponent(providedType, dependencyDescriptor)) {
251         providedClass.isAssignableFrom(List.class) || providedClass.isAssignableFrom(List.class)
    }
252     continue;
253 }
```

A "NullPointerException" could be thrown; "providedClass" is nullable here.

Bug Major cert, cwe



Код уже написан

A Что такое Shift-Left Security?



Планирование

Проектирование и дизайн

Реализация

Тестирование

Эксплуатация

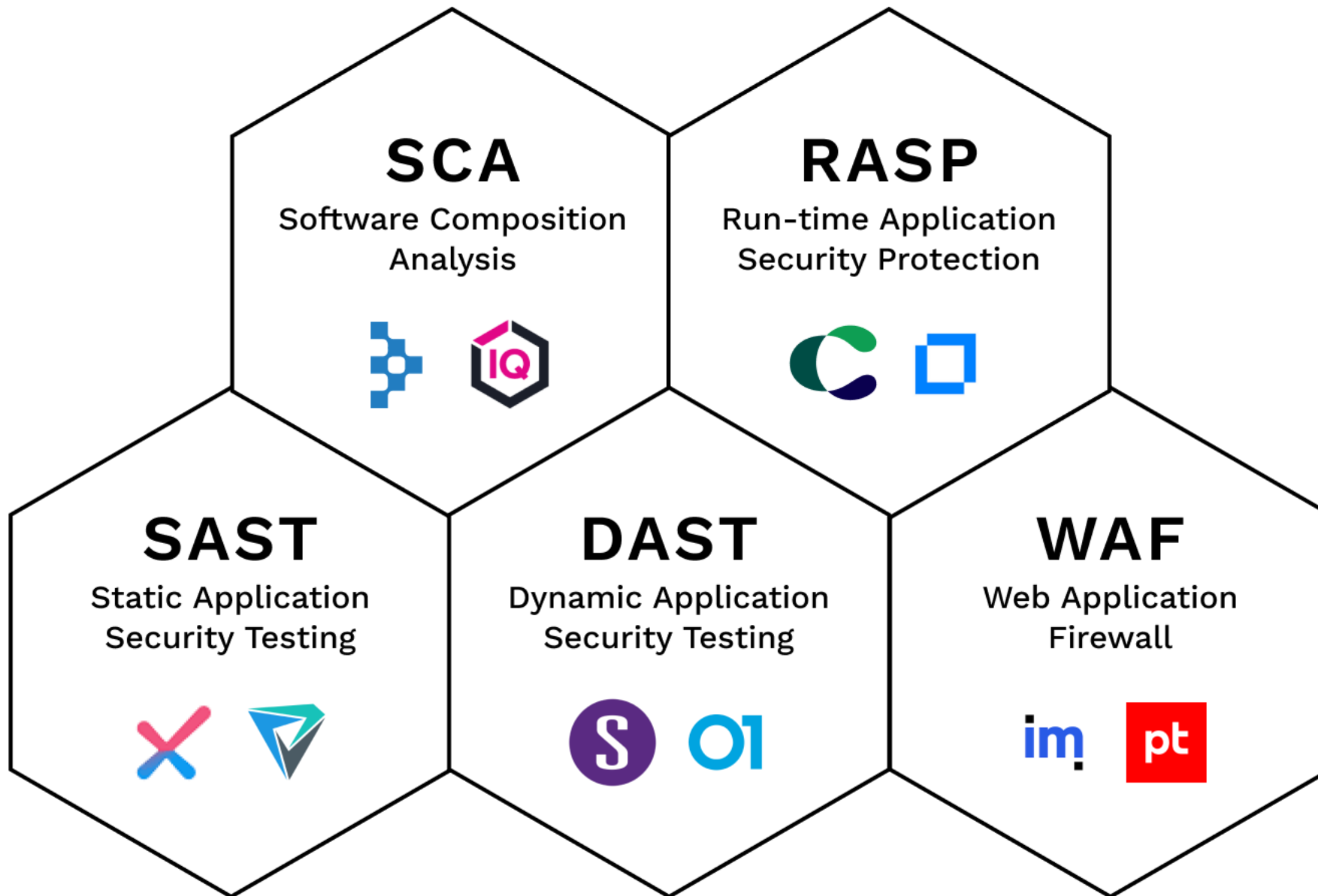


A

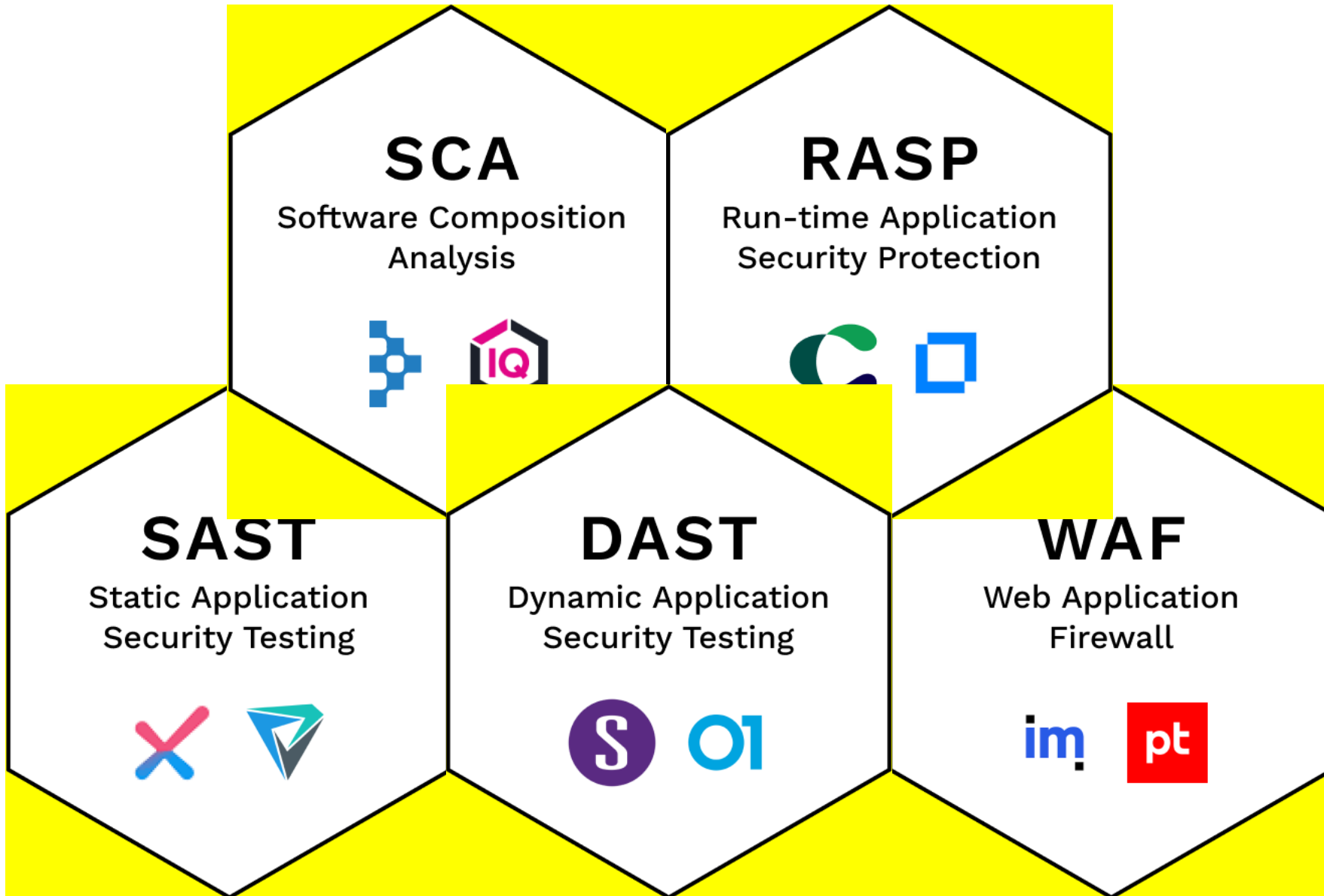
Относительная стоимость устранения дефектов ПО на разных этапах разработки



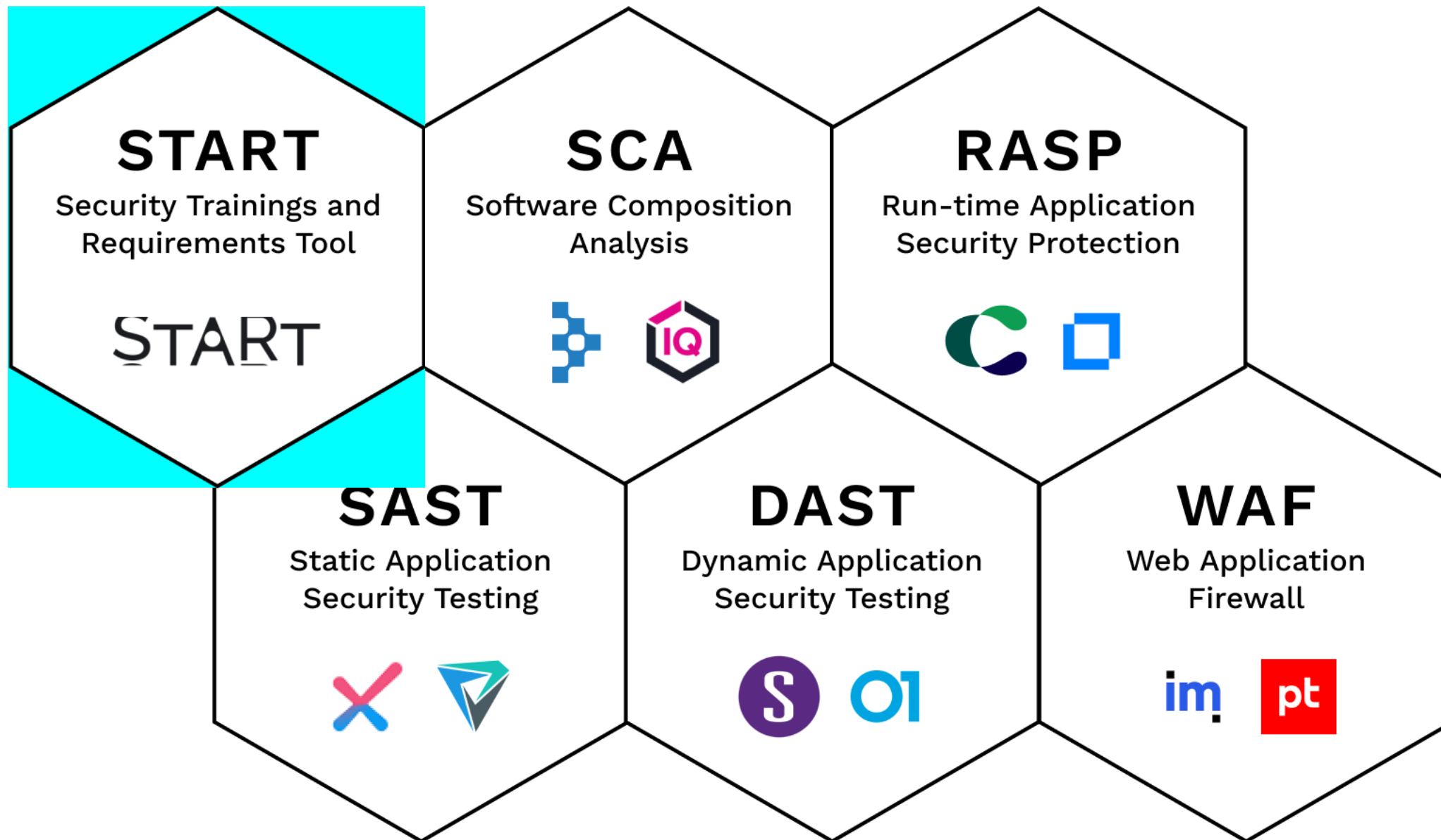
A Какие инструменты делают продукт безопасным?



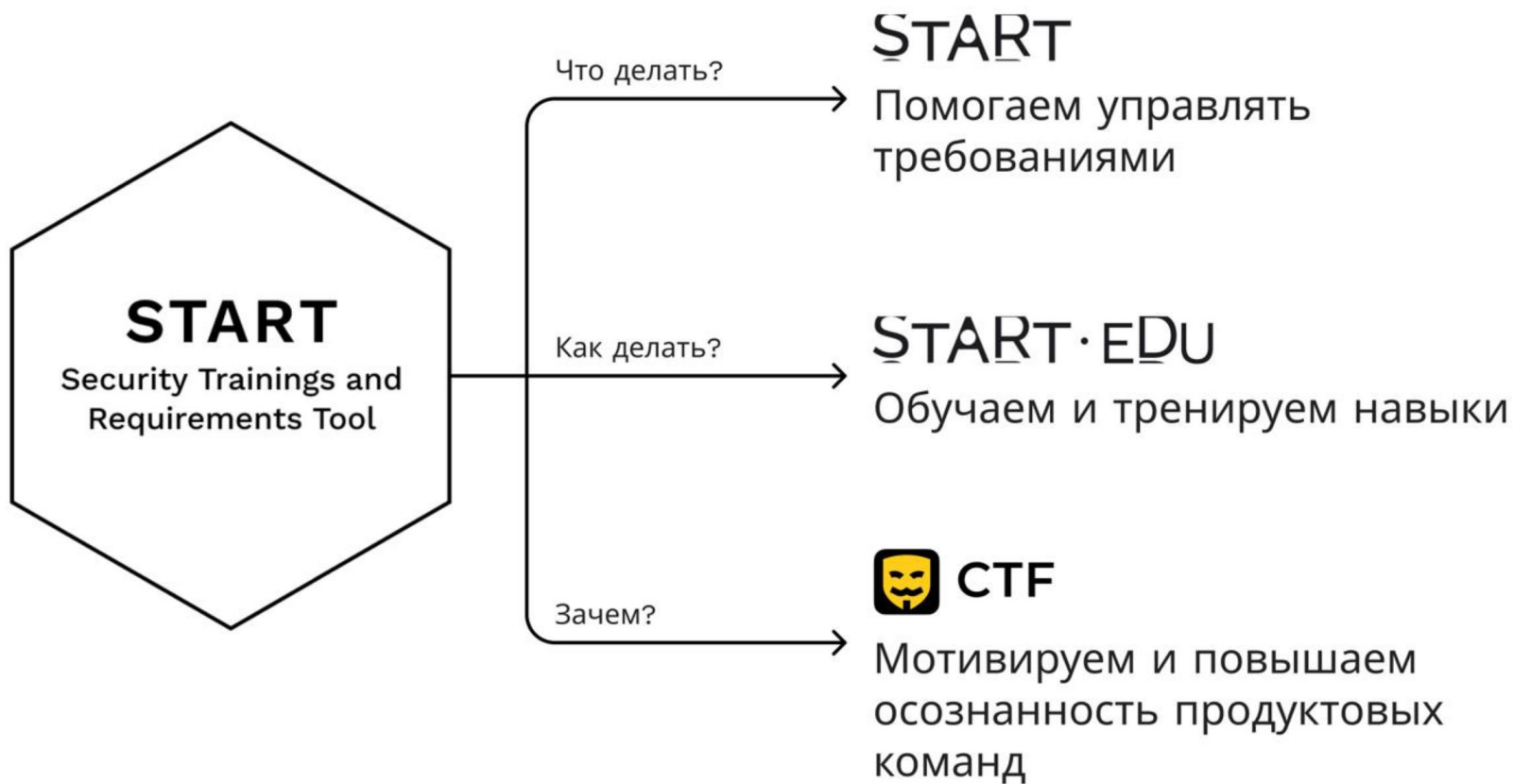
A Инструменты не делают продукт безопасным



A Люди делают продукт безопасным



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



A 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, предотвращающих утечку информации путем использования программного обеспечения.



При наличии технических средств защиты информации оператор по переводу денежных средств, банковский платежный агент (субагент), оператор услуг платежной инфраструктуры 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.



А 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, и



- действителен на протяжении установленного периода времени;
- используется для подтверждения права доступа к системе Интернет-банкинга (распоряжения (нескольких распоряжений) о распоряжениях (нескольких переводах) денежных средств или распоряжения о переводах денежных средств в определенную дату или в течение определенного периода времени);
- 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



A Антифишинг. START для продуктовых команд

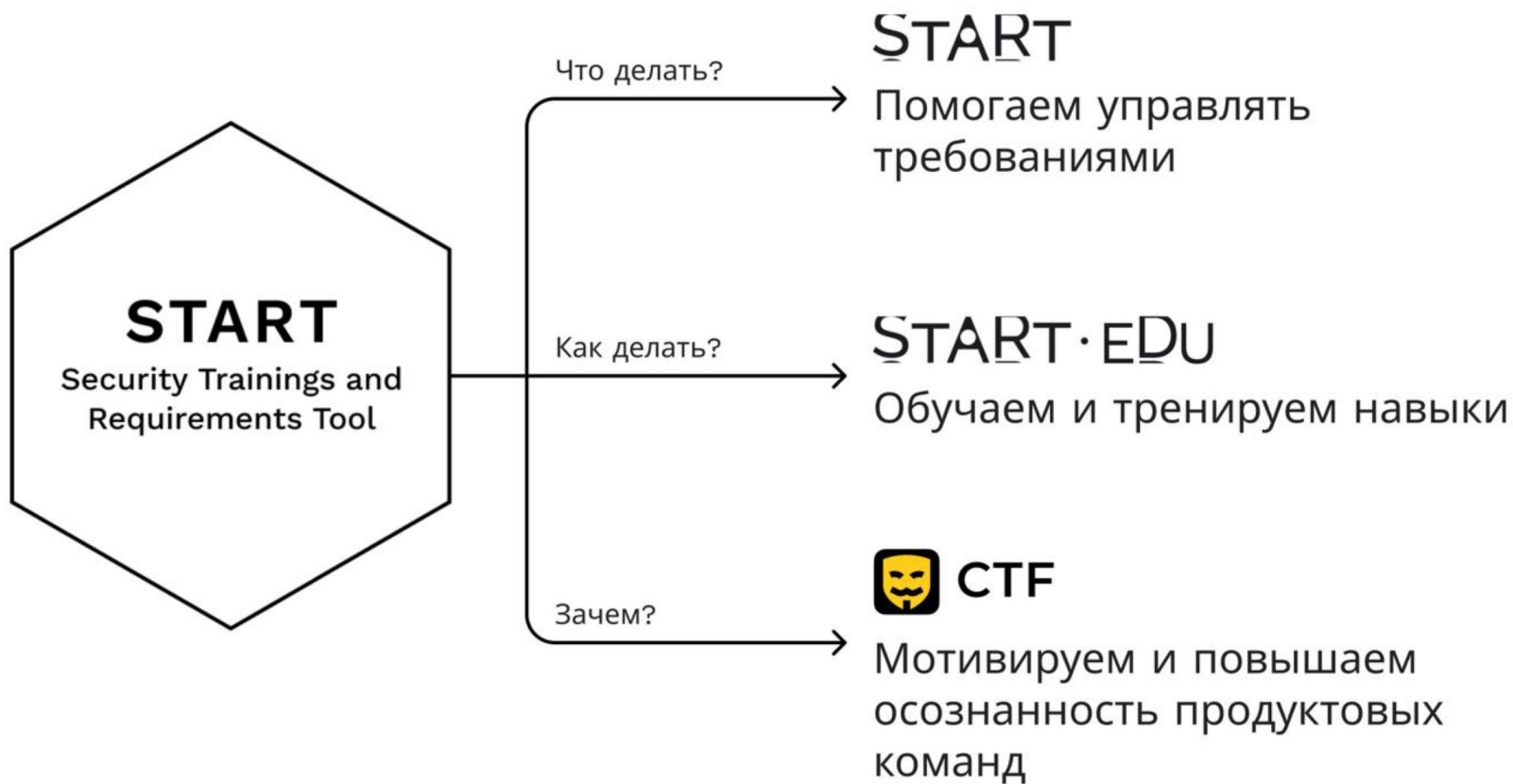
Первое решение класса ASRTM (Application security requirements and threat management) на российском рынке.

Приложение № 1 к Протоколу испытания на соответствие требованиям

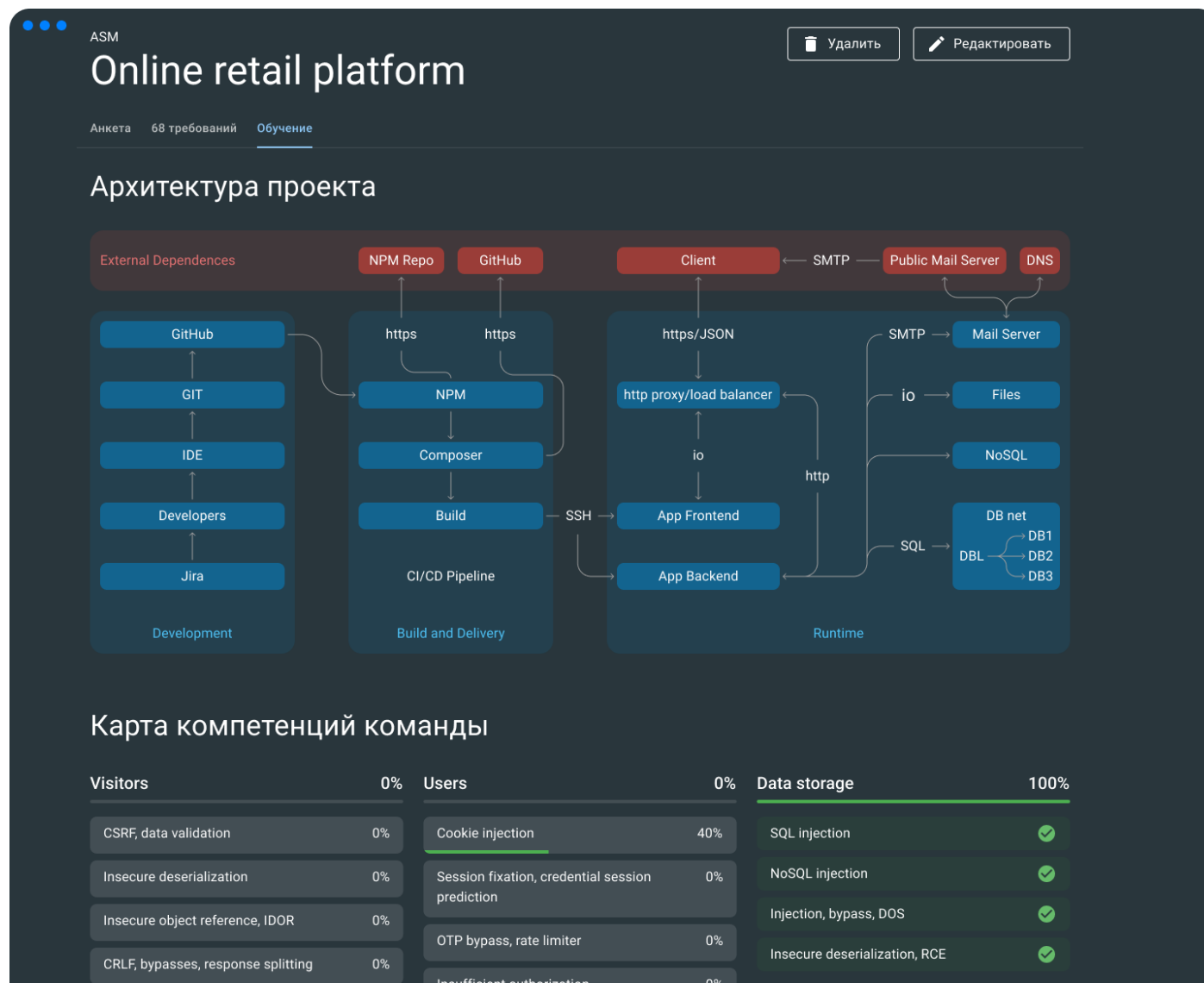
| № п/п | Код | Формулировка требования | Результат испытания и замечания | Критичность | Срок устранения замечания |
|-------|-----|---|---------------------------------|-------------|---------------------------|
| 1 | AR | Архитектура и Дизайн | | | |
| 2 | AR3 | Для взаимодействия с другими приложениями и компонентами должны использоваться учетные записи, обладающие минимально необходимыми полномочиями. | Без замечаний | Средняя | |
| 3 | CO | Технические. Общие требования и документирование | | | |
| 4 | CO1 | В документации на приложения должны быть перечислены все используемые криптографические библиотеки, цели и способы их | Без замечаний | Высокая | |

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

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



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



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

The screenshot shows a user profile for Алексей Рыбаков, a frontend developer. It features progress bars for 'Системы' (Systems) and 'Карта компетенций' (Competency Map). The 'Системы' section shows progress for 'CTF' (0/10) and 'START' (2/10). The 'Карта компетенций' section includes a search bar and a table of skills with progress indicators.

Алексей Рыбаков

Фронтенд-разработчик

250 Новичок

Системы

- CTF**
Пройшел 0/10
- START**
Пройшел 2/10
- LMS**
Пройшел 0/10

Show more ▾

Карта компетенций

Название контекста или юнита | Показывать Все

| Visitors | 0% | Users | 11% | Data st |
|------------------------------------|--------|--|-------|-----------|
| CSRF, data validation | +100 ★ | Cookie injection | 45 ✓ | SQL inj |
| Insecure deserialization | +100 ★ | Session fixation, credential session prediction | 45 ✓ | NoSQL |
| Insecure object reference, IDOR | +100 ★ | OTP bypass, rate limiter | +50 ★ | Injection |
| CRLF, bypasses, response splitting | +100 ★ | Insufficient authorization | +50 ★ | Insecu |
| Insufficient anti-automation | +100 ★ | Insecure password checks | +50 ★ | |
| Insecure parsing and reference | +50 ★ | Weak password recovery validation, host header injection | +50 ★ | |
| XXE, xpath injection | +50 ★ | | | |

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

злоумышленник не располагает этой информацией.

Предположим, что у нас есть веб-приложение, в котором сессии хранятся в cookie, а пользователи могут изменить свой адрес электронной почты с помощью следующей HTML-формы:

```
HTML-form
1 <html>
2   <body>
3     <form action="/user/email" method="POST">
4       <input type="email" name="email" value="" />
5       <input type="submit">
6     </form>
7   </body>
8 </html>
```

Если пользователь введет новый адрес в форму и нажмет «Сохранить», его браузер отправит POST-запрос, содержащий данные из формы:

```
HTML-form
1 POST **/user/email** HTTP/1.1
2 Host: example.com
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 22
5 **Cookie: PHPSESSID=JKcciBhFZ0tTp1xh7QW2DigRqdUZknbC**
6
7 **email=user@example.com**
8
```

Проанализировав запрос, потенциальный злоумышленник обнаружит, что он соответствует условиям для проведения успешной CSRF-атаки:

1. Действие по изменению адреса электронной почты в учетной записи пользователя представляет интерес для злоумышленника:

Защита от подд
запросов: CSRF

Теория

- ✓ Зачем этот курс
- ✓ Что такое CSRF
- 🔖 Как происходит
- 🔖 Как защититься
- 🔖 Частые вопросы

Квиз

Практика

Шаг 4. Теория и примеры кода

Сотрудники получают доступ к учебным модулям гибридной структуры



Предположим, что у нас есть веб-приложение, в котором пользователи могут изменить свой адрес электронной почты, а пользователи могут изменить свой адрес электронной почты с помощью следующей HTML-формы:

HTML-form

```
1 <html>
2   <body>
3     <form action="/user/email" method="POST">
4       <input type="email" name="email" value="" />
5       <input type="submit" value="Изменить" />
6     </form>
7   </body>
8 </html>
9
```

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

HTML-form

```
1 POST **/user/email** HTTP/1.1
2 Host: example.com
3 Content-Type: application/x-www-form-urlencoded
4 Content-Length: 22
5 **Cookie: PHPSESSID=JKeeiPbE70+Tn1xk70W2DgRed
```

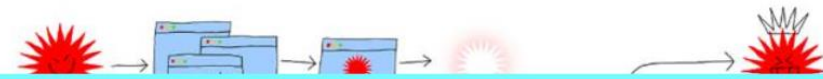
Как происходит CSRF-атака

Защита от подделанных запросов – CSRF

Теория

☑ Зачем этот CSRF

☑ Что такое CSRF



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

```
1 @Override
2 protected void configure(HttpSecurity http) throws Exception {
3     http.csrf().disable();
4 }
5
```

Шаг 6. Практика ревью кода



The screenshot displays a code review interface for a file named `app.py`. The interface is split into three main sections:

- Project Sidebar:** Shows the file structure with `app.py` selected. Other files include `.git`, `templates`, `Dockerfile`, and `requirements.txt`.
- Code Editor:** Shows a diff between two versions of `app.py`. The code includes imports for `Flask`, `Response`, `abort`, `redirect`, `render_template`, `request`, `url_for`, `flask_login` (LoginManager, UserMixin, current_user, login_required, login_user, logout_user), `flask_wtf.csrf`, and a database configuration.
- Review Bar:** A horizontal bar at the bottom of the diff view contains three options: **Option 1**, **Option 2**, and **Option 3**. To the right of these options are two buttons: **Approve** (with a green checkmark) and **Deny** (with a red X).

```
1 from flask import Flask, Response, abort, redirect,
2   render_template, request, url_for
3 from flask_login import
4   LoginManager, UserMixin, current_user, login_required,
5   login_user, logout_user
6 from flask_wtf.csrf import CSRFProtect
7
8 app = Flask(__name__)
9 app.config.update(
10     DEBUG=True,
11     SECRET_KEY="secret_antiCSRF",
12 )
13
14 login_manager = LoginManager()
15 login_manager.init_app(app)
16
17 csrf = CSRFProtect()
18 csrf.init_app(app)
19
20 # database
21 users = [
22     {
```

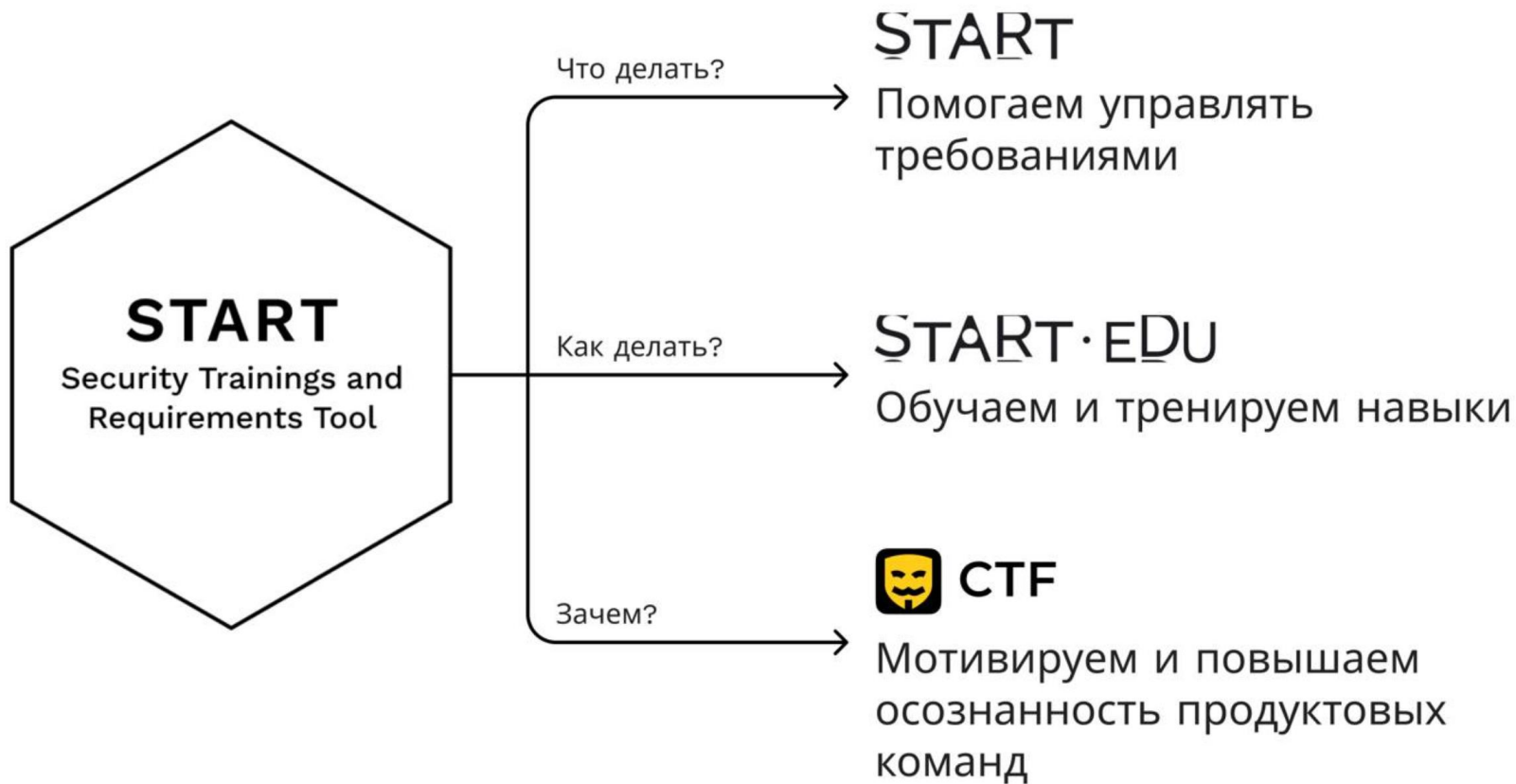
Шаг 7. Практика с написанием кода, Q2 2023



```
Discard all changes Run code
Project app.py
> .git
> templates
app.py
Dockerfile
requirements.txt
68     if user["username"] == username and user["password"] == password:
69         user_model = User()
70         user_model.id = user["id"]
71         login_user(user_model)
72         return redirect(url_for("accounts"))
73     return abort(401)
74
75     if current_user.is_authenticated:
76         return redirect(url_for("accounts"))
77
78     return render_template("index.html")
79
80
81 @app.route("/accounts", methods=["GET", "POST"])
82 @login_required
83 def accounts():
84     user = get_user(current_user.id)
85     data = {**request.args, **request.form}
86
87     if data:
88         amount = int(data['amount'])
89         account = int(data['account'])
90         transfer_to = get_user(account)
91
92         if amount <= user["balance"] and transfer_to:
```

▶ Run code

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



START.CTF



Тренажер по практической безопасности в формате действующего интернет-банка

HackMeBank Банк Блог Помощь USD 104,15 P EUR 144,85 P Войти ↗

Мультивалютная электронная карта от HackMeBank

Зарабатывайте деньги, а не бонусы. Закажите карту с кэшбэком до 6% и ежемесячным процентом на остаток

Получить карту

HackMeBank
0000 0000 0000 0000
01/29
KONSTANTIN IVANOV

Изменить

Закрыть

| | |
|--------------|-------------------|
| Me *0881 | 1 253,73 |
| и | 14:05:01 |
| Me USD *0882 | 2000,00 → \$34,24 |
| и | 17:02:28 |

О карте

START.CTF



Тренажер по практической безопасности в формате действующего интернет-банка

Поиск и эксплуатация уязвимостей

| | | | |
|-----------------------|-------------------------------|--------------------------------|--------------------------|
| Обход OTP 500 | Положительный баланс 500 | Подозрительные операции 500 | Постоянный клиент 500 |
| Важные новости 500 | Пора платить по счетам 500 | | |

XSS Challenge

| | |
|---------------|--------------|
| XSS 1 100 | XSS 2 100 |
| XSS 11 150 | XSS 5 200 |

Challenge 0 Solves ×

XSS 2

100

В этом задании вам необходимо найти и проэксплуатировать XSS. <http://xss-challenge.hackmebank.ru/challenge2.html>

Для получения флага - отправьте url, при переходе по которой выполнится команда `alert(1337)`, в форму по ссылке: <http://xss-challenge.hackmebank.ru:8000/>

Flag

Submit



4 недели

длится соревнование

A Вопросы про безопасность — продвинутый уровень



— Аутентификация при межсервисном взаимодействии работает очень медленно, лучше без нее?

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



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



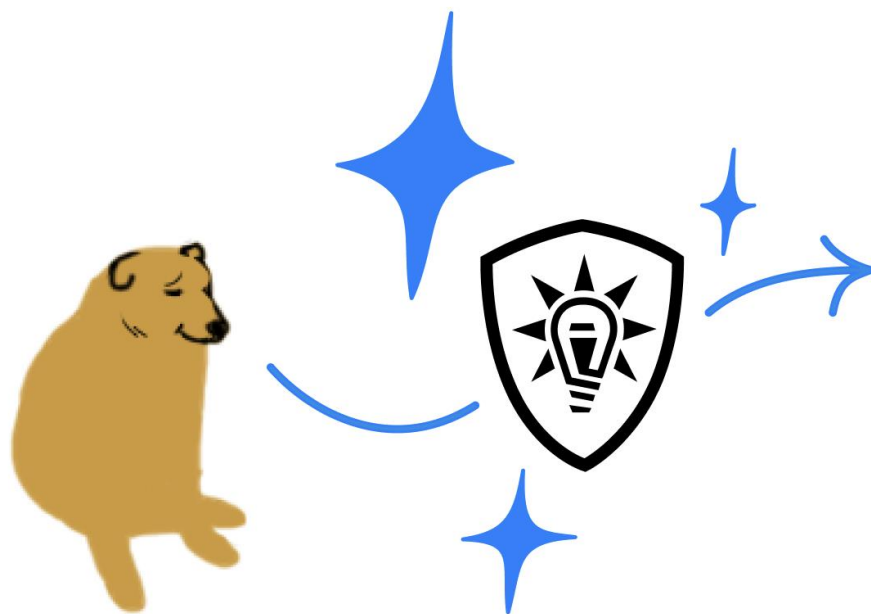
Ответы сотрудников на такие вопросы – и есть культура безопасности компании

A 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 партнера, парт стороны перед решил попракт И во время ана. обратный прок обращался к lo Оказалось, что видимо кто-то 2007 году встрс



ОДНОМ ИЗ
ЭТИЛИ
КОМПАНИЯ
ИХ
Е ТОЛЬКО

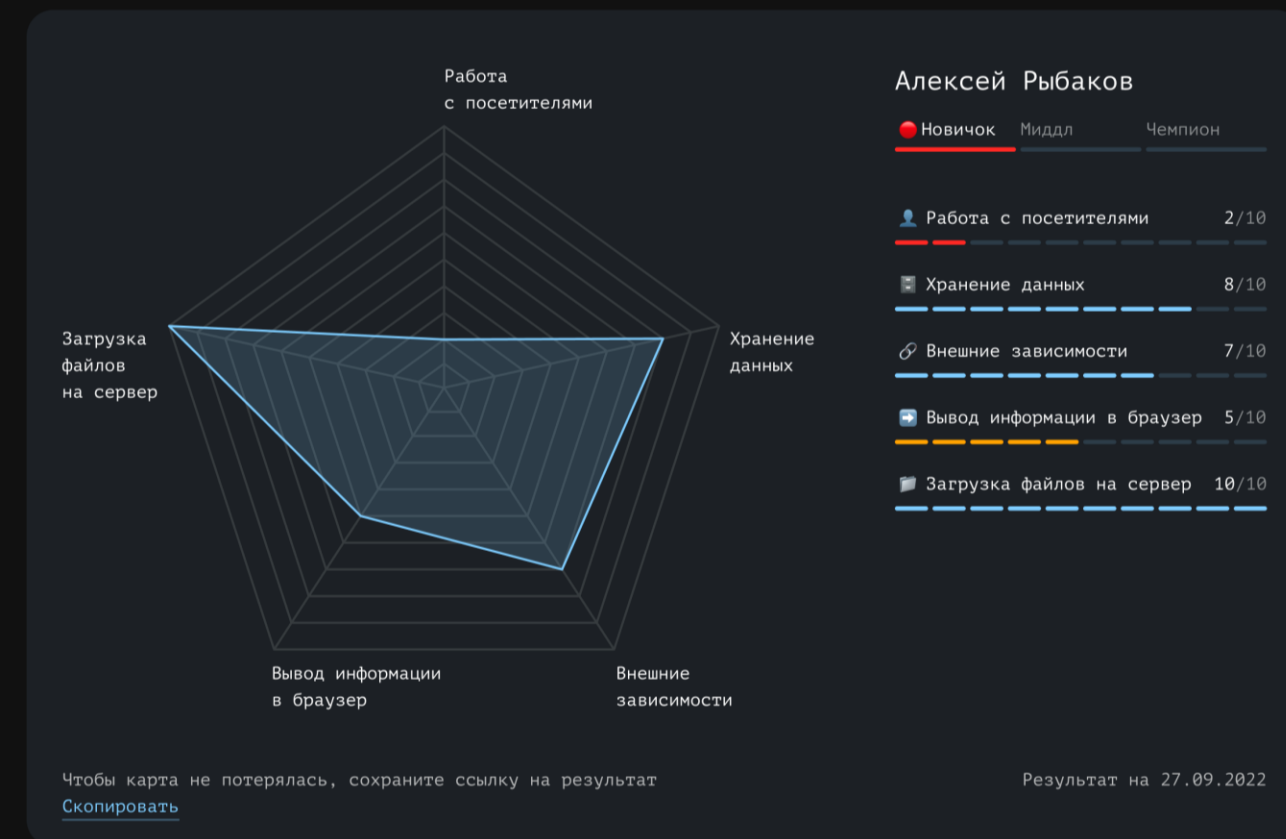
Тест для продуктовых команд

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



A Продукты «Антифишинга» уже используют



М.ВидеоЭльдорадо



START



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

