SOC
FORUM
2024

Браузер пользователя как источник событий для SOC. Как начать видеть в «слепой» зоне?

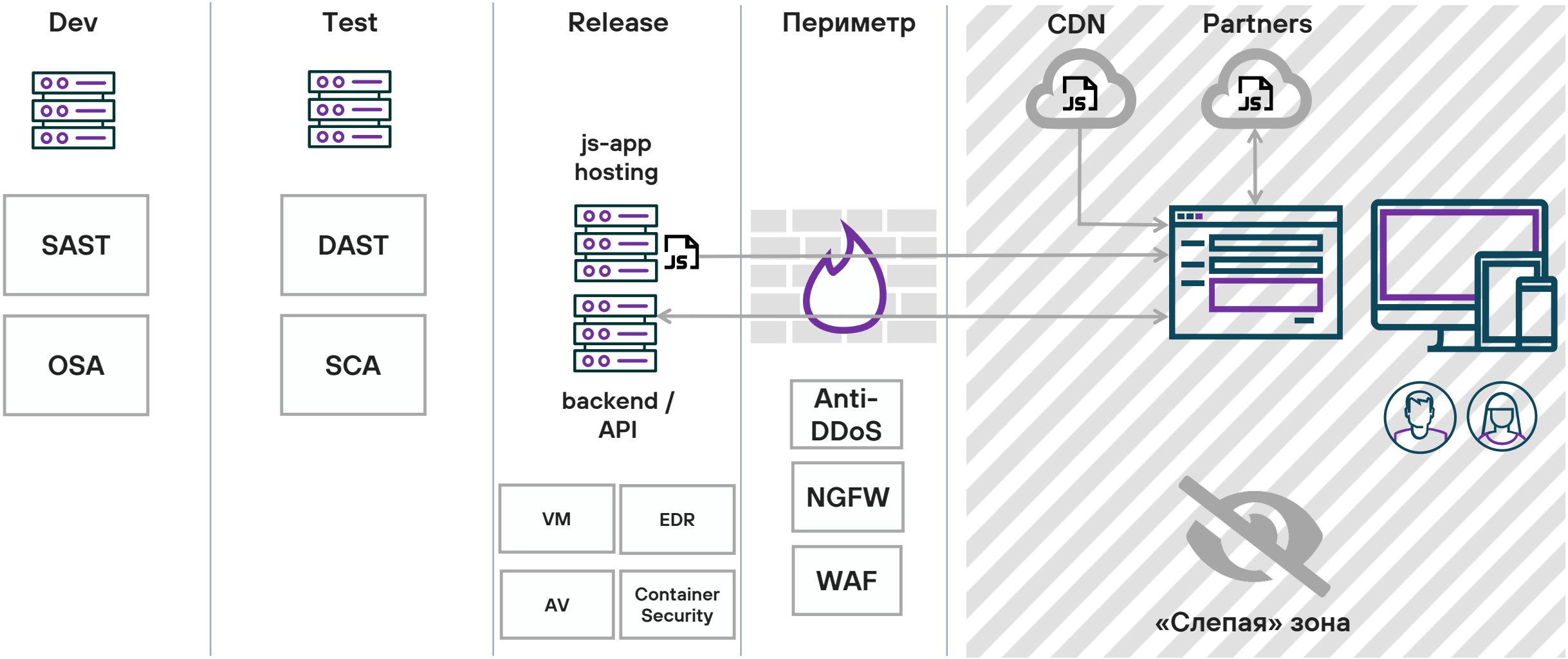
SOC
FORUM
2024

Михаил Парфенов

DPA Analytics

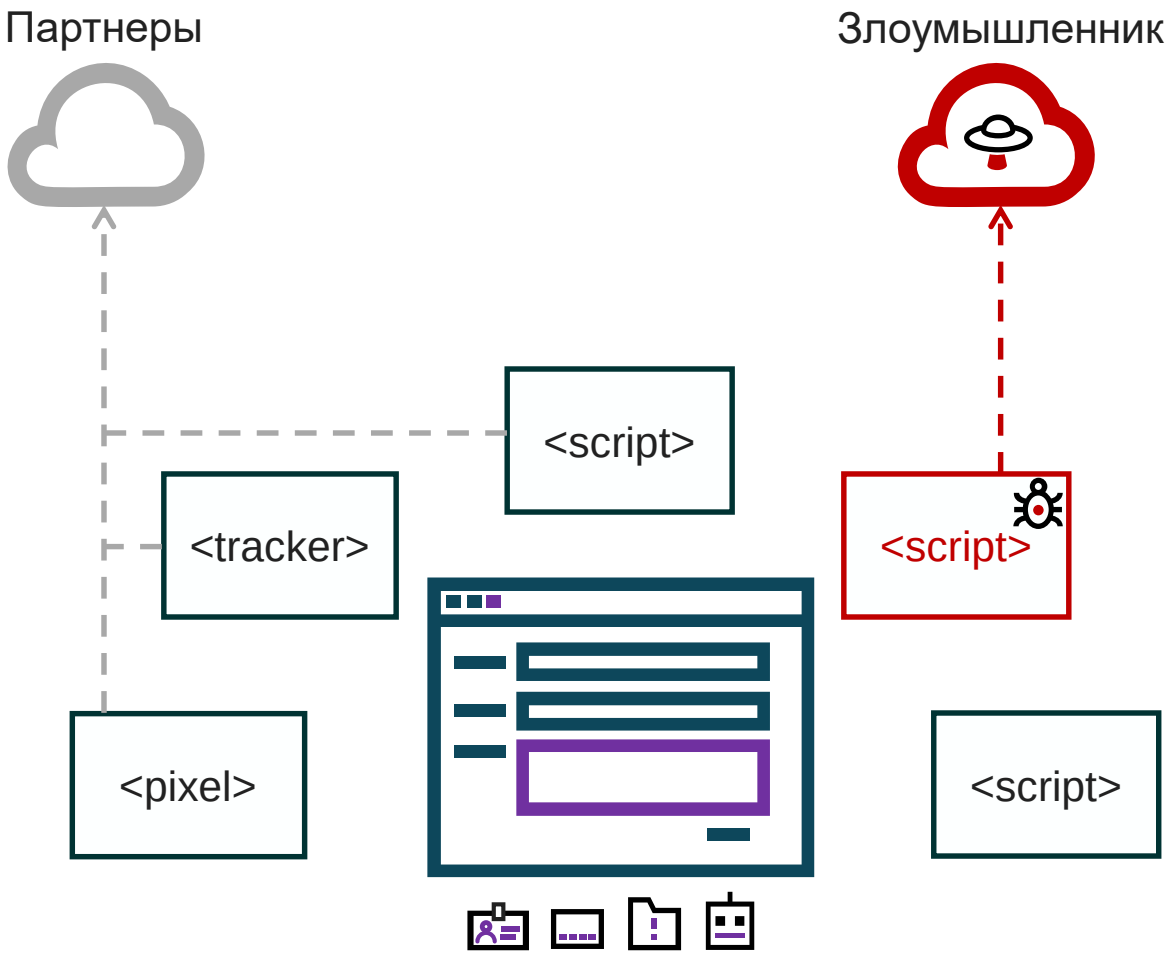
Безопасность веб-приложений

SOC FORUM 2024



Ценность frontend-приложений для злоумышленника

SOC FORUM 2024



- Данные (персональные, банковские карты, учетные записи)
- Цифровой отпечаток устройства пользователя / установка cookie
- Выполнение действий от имени
- Показ пользователю мошеннических баннеров от имени компании для последующей кражи денег / данных
- Майнинг криптовалюты в браузере пользователя либо использование браузера в DDoS-атаках на другие ресурсы
- Заражение устройства пользователя через уязвимости браузера

Основные компоненты frontend-приложения

SOC FORUM 2024

JS-приложение и его зависимости

- Код фреймворка
- Собственный код
- Прямые зависимости
- Транзитивные зависимости

Как правило, перед публикацией приложения собираются в единый файл-bundle

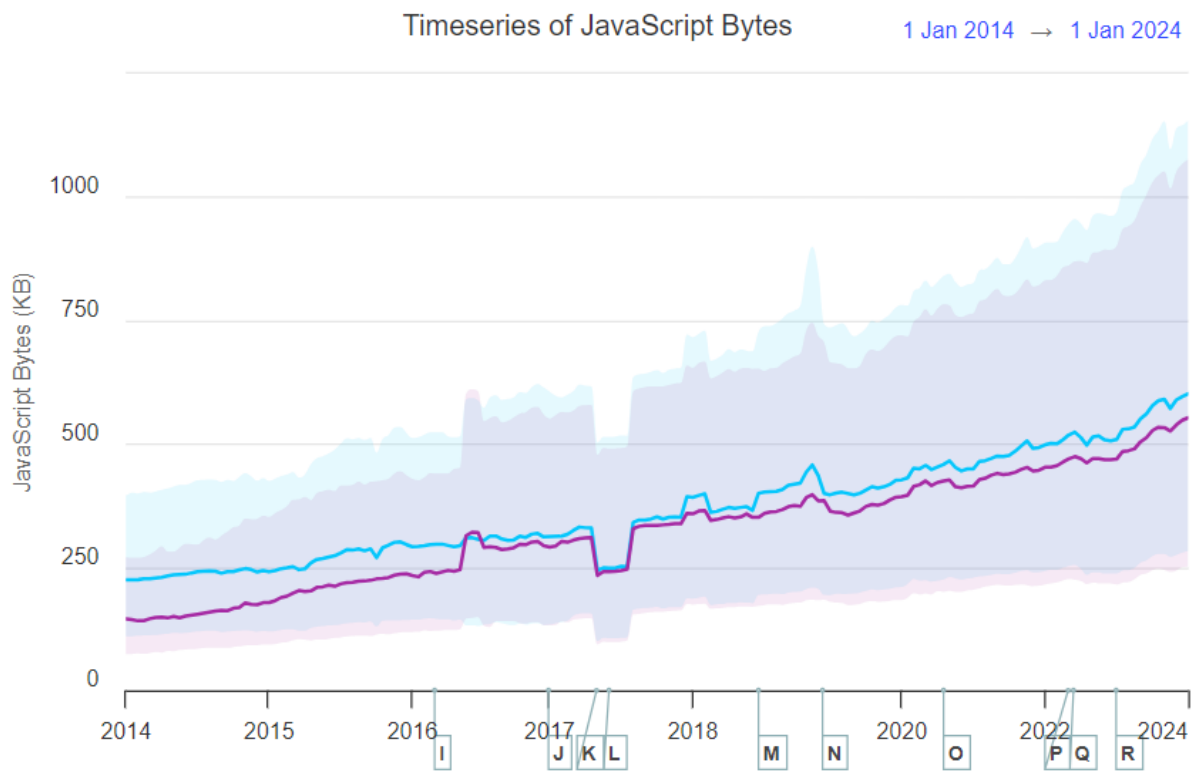
Сторонние JS-сервисы

- Сервисы веб-аналитики
- Интернет-счетчики
- Маркетинговые системы
- Платформы контекстной рекламы
- Captcha
- Онлайн-чаты
- Онлайн-карты
- JS-библиотеки во внешних CDN
- И другие

Размер JavaScript-приложений

SOC FORUM 2024

Веб-приложение	Размер JS-файлов
Jira Cloud	50 МБ
mail.google.com	20 МБ
1Password.com	13 МБ
gitlab.com	13 МБ
YouTube	12 МБ
Google.com	9 МБ
ChatGPT	7 МБ
Npmjs.com	4 МБ
StackOverflow	3,5 МБ
wikipedia.org	0,2 МБ

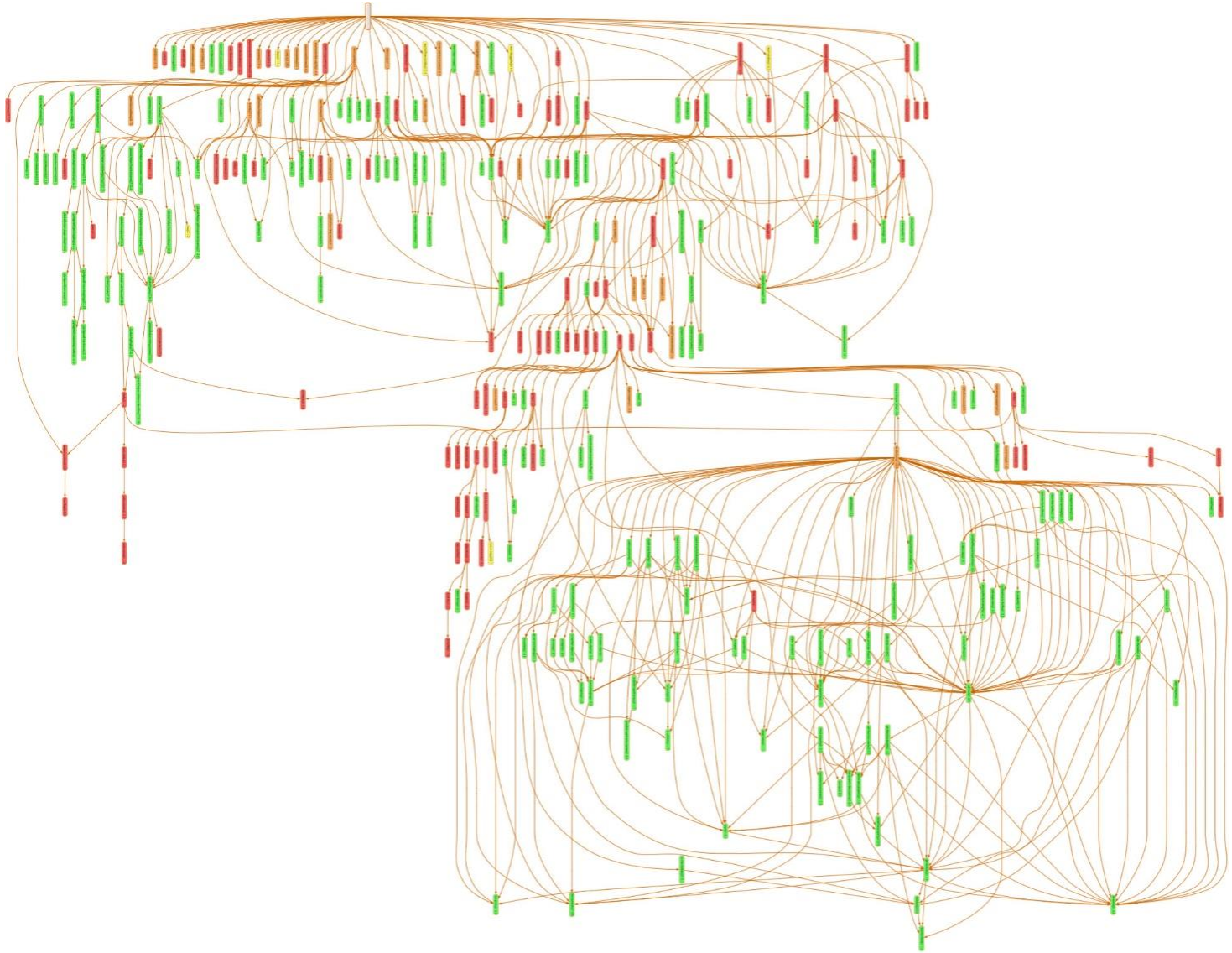


https://habr.com/ru/companies/ruvds/articles/796595/

https://httparchive.org

Зависимости в JavaScript-приложениях

SOC FORUM 2024



Количество

94

Глубина

15

Размер (МБ)

12

Минификация и обфускация

SOC FORUM 2024

```
!function(e,t){"use strict";"object"==typeof module&&"object"==typeof module.exports?module.export
window with a document");return t(e)}:t(e)}("undefined"!=typeof window?window:this,function(ie,e)
ae=oe.slice,g=oe.flat?function(e){return oe.flat.call(e)}:function(e){return oe.concat.apply([],e)
ue=n.hasOwnProperty,o=ue.toString,a=o.call(Object),le={},v=function(e){return"function"==typeof e
null!=e&&e===e.window},C=ie.document,u={type:!0,src:!0,nonce:!0,noModule:!0};function m(e,t,n){var
u)(i=t[r]||t.getAttribute&&t.getAttribute(r))&&o.setAttribute(r,i);n.head.appendChild(o).parentNod
e||"function"==typeof e?n[i.call(e)]||"object":typeof e}var t="3.7.1",l=/HTML$/i,ce=function(e,t)
e&&e.length,n=x(e);return!v(e)&&!y(e)&&("array"===n||0===t||"number"==typeof t&&0<t&&t-1 in e)}fun
===t.toLowerCase()}ce.fn=ce.prototype={jquery:t,constructor:ce,length:0,toArray:function(){return
null==e?ae.call(this):e<0?this[e+this.length]:this[e]},pushStack:function(e){var t=ce.merge(this.
ce.each(this,e)}, map:function(n){return this.pushStack(ce.map(this,function(e,t){return n.call(e,
this.pushStack(ae.apply(this,arguments))},first:function(){return this.eq(0)},last:function(){retu
this.pushStack(ce.grep(this,function(e,t){return(t+1)%2}))},odd:function(){return this.pushStack(
t=this.length,n=+e+(e<0?t:0);return this.pushStack(0<=n&&n<t?[this[n]]:[])},end:function(){return
oe.splice},ce.extend=ce.fn.extend=function(){var e,t,n,r,i,o,a=arguments[0]||{},s=1,u=arguments.le
a||v(a)||(a={}),s===u&&(a=this,s--);s<u;s++)if(null!=(e=arguments[s]))for(t in e)r=e[t],"__proto__
a[t],o=i&&!Array.isArray(n)?[]:i||ce.isPlainObject(n)?n:{},i=!1,a[t]=ce.extend(l,o,r)):void 0! ==
)).replace(/\D/g,""),isReady:!0,error:function(e){throw new Error(e)},noop:function(){},isPlainObj
Object]"!==i.call(e))&&(!(t=r(e))||"function"== typeof(n=ue.call(t,"constructor")&&t.constructor)&
e)return!1;return!0},globalEval:function(e,t,n){m(e,{nonce:t&&t.nonce},n)},each:function(e,t){var
in e)if(!1===t.call(e[r],r,e[r]))break;return e},text:function(e){var t,n="",r=0,i=e.nodeType;if(
1===i||11===i?e.textContent:9===i?e.documentElement.textContent:3===i||4===i?e.nodeValue:n},makeAr
null!=e&&(c(Object(e))?ce.merge(n,"string"==typeof e?[e]:e):s.call(n,e)),n},inArray:function(e,t,r
t=e&&e.namespaceURI,n=e&&(e.ownerDocument||e).documentElement;return!l.test(t||n&&n.nodeName||"HTM
n=+t.length,r=0,i=e.length;r<n;r++)e[i++]=t[r];return e.length=i,e},grep:function(e,t,n){for(var
r},map:function(e,t,n){var r,i,o=0,a=[];if(c(e))for(r=e.length;o<r;o++)null!=(i=t(e[o],o,n))&&a.pu
g(a)},guid:1,support:le}),"function"==typeof Symbol&&(ce.fn[Symbol.iterator]=oe[Symbol.iterator]),
Symbol".split(" "),function(e,t){n["[object "+t+"]"]=t.toLowerCase()});var pe=oe.pop,de=oe.sort,he
RegExp("^"+ge+"+|((?:^|[^\\\\])(?:\\\\.)*)"+ge+"+$","g");ce.contains=function(e,t){var n=t&&t.pare
e===n||!(!n||1!==n.nodeType||!(e.contains?e.contains(n):e.compareDocumentPosition&&16&e.compareDoc
p(e,t){return t?"\0"===e?"\ufffd":e.slice(0,-1)+"\\"+e.charCodeAt(e.length-1).toString(16)+" ":"\
ye=C,me=s;!function(){var e,b,w,o,a,T,r,C,d,i,k=me,S=ce.expando,E=0,n=0,s=W(),c=W(),u=W(),h=W(),l=
e===t&&(a=!0),0},f="checked|selected|async|autofocus|autoplay|controls|defer|disabled|hidden|ismap
[^\\r\\n\\f]|[\\w-]|[^\0-\\x7f])+",p="\\["+ge+"*("+t+")(?:"+ge+"*([*^$|!~]?=)"+ge+"*(?:'((?:\\\\.
?:\\\\.|[^\\\\'])*)'|\"((?:\\\\.|[^\\\\\"])*)\"|((?:\\\\.|[^\\\\()[\\]]|"+p+")*)|.*)\\)|)",v=new
```

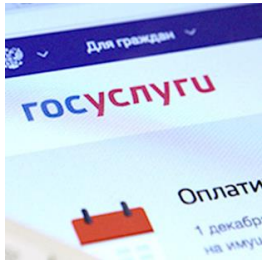
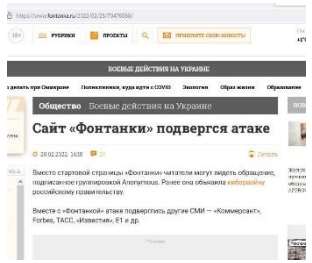
Frontend-приложения

SOC FORUM 2024

1. Работают в «слепой» зоне для ИБ
2. Средства защиты и анализаторы ИБ не обнаруживают актуальные угрозы
3. Время присутствия вредоносного кода – недели / месяцы в известных инцидентах
4. Часто игнорируются ИБ-специалистами
5. Максимальная монетизация для злоумышленника

Инциденты

SOC FORUM 2024

			Magento	Google Tag Manager		Polyfill.io
Год	**2017**	**2018**	**2019**	**2021**	**2022**	**2024**
Инцидент	Размещены iframe с неизвестными доменами в Нидерландах	Злоумышленник встроил в одну из js-библиотек js-сниффер	В 100 000+ интернет-магазинов встроен js-сниффер	В 316 интернет-магазинах обнаружен js-сниффер, скрытый в Google Tag Manager	Внедрен код на сайты СМИ «Коммерсантъ», Forbes, РБК, ТАСС, «Известия», крупных банков и других	Внедрен вредоносный код в библиотеку Polyfill.js. Код выполнялся на > 380 000 веб-приложений.
Вектор	N/A	Взлом через уязвимость	Взлом через уязвимость в CMS Magento	Уязвимости CMS: WordPress, Shopify, BigCommerce	Взломан внешний сервис статистики onthe.io, изменен код js-скрипта	Supply chain attack. Код внедрен владельцами библиотеки.
Время присутствия	N/A	15 дней	5 месяцев	N/A	1-3 дня	> 4 месяцев
Последствия	N/A	Похищены данные банковских карт 380 000 клиентов	Похищены персональные данные клиентов (1.5 млн посетителей / день), банковские карты 500 000 клиентов.	Похищены данные банковских карт	Неработоспособность ресурсов. Политические лозунги на страницах.	Редирект пользователей мобильных устройств на сайты онлайн-букмекеров.
Ущерб	N/A Устранено через 4 часа после публикации статьи Dr. Web	2 280 000 000 £ + штраф 20 000 000 £ по GDPR		N/A	N/A	N/A Неработоспособность сайтов после блокировки домена.

Что необходимо видеть?

SOC FORUM 2024

1

Скрипты и другие активные элементы

2

Сетевые запросы, выполняемые js-приложением в браузере

3

API-браузера, используемое js-приложением

Единственное место, где можно обнаружить изменения и признаки вредоносной активности – это браузер пользователя, где страница полностью собрана и выполнен весь JavaScript-код

PCI DSS 4.0.1

Источники событий

SOC FORUM 2024

1. Content Security Policy (CSP)
2. Frontend Sandbox
3. Frontend Observability

Content Security Policy (CSP)

SOC FORUM 2024

HTTP-заголовок Content-Security-Policy-Report-Only

- Подойдет в качестве базового источника событий
- Включение report-to генерирует значительный объем запросов. Необходимо принимать, анализировать, применять правила корреляции
- Контролирует не все каналы передачи данных в браузере
- Злоумышленник может отключить/изменить CSP при взломе сервера
- Не контролирует состав отправляемых скриптами данных
- Не контролирует поведение скриптов (в том числе в зависимостях)
- Отдельная CSP для фреймов

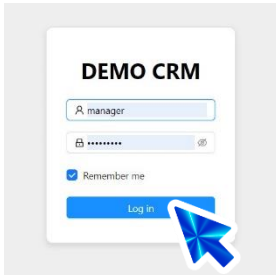
Статья «Content Security Policy (CSP) защитит от js-снифферов и утечек?»

Frontend Sandbox
Frontend Application Security Testing (FAST)

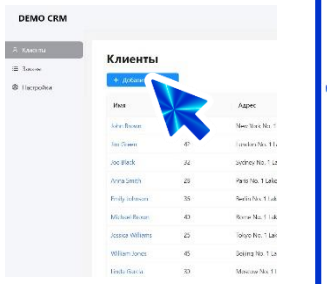
SOC FORUM 2024

Открытие страницы

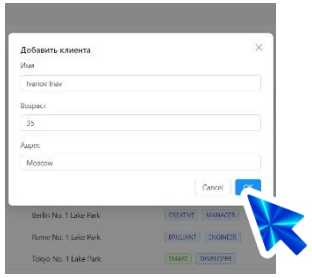
Ввод логина, пароля, клик по кнопке



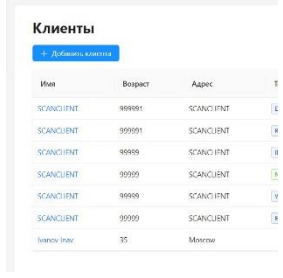
Успешная аутентификация, редирект



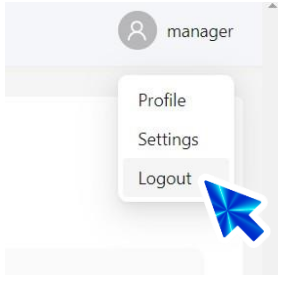
Открытие формы создания клиента, заполнение данных



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.

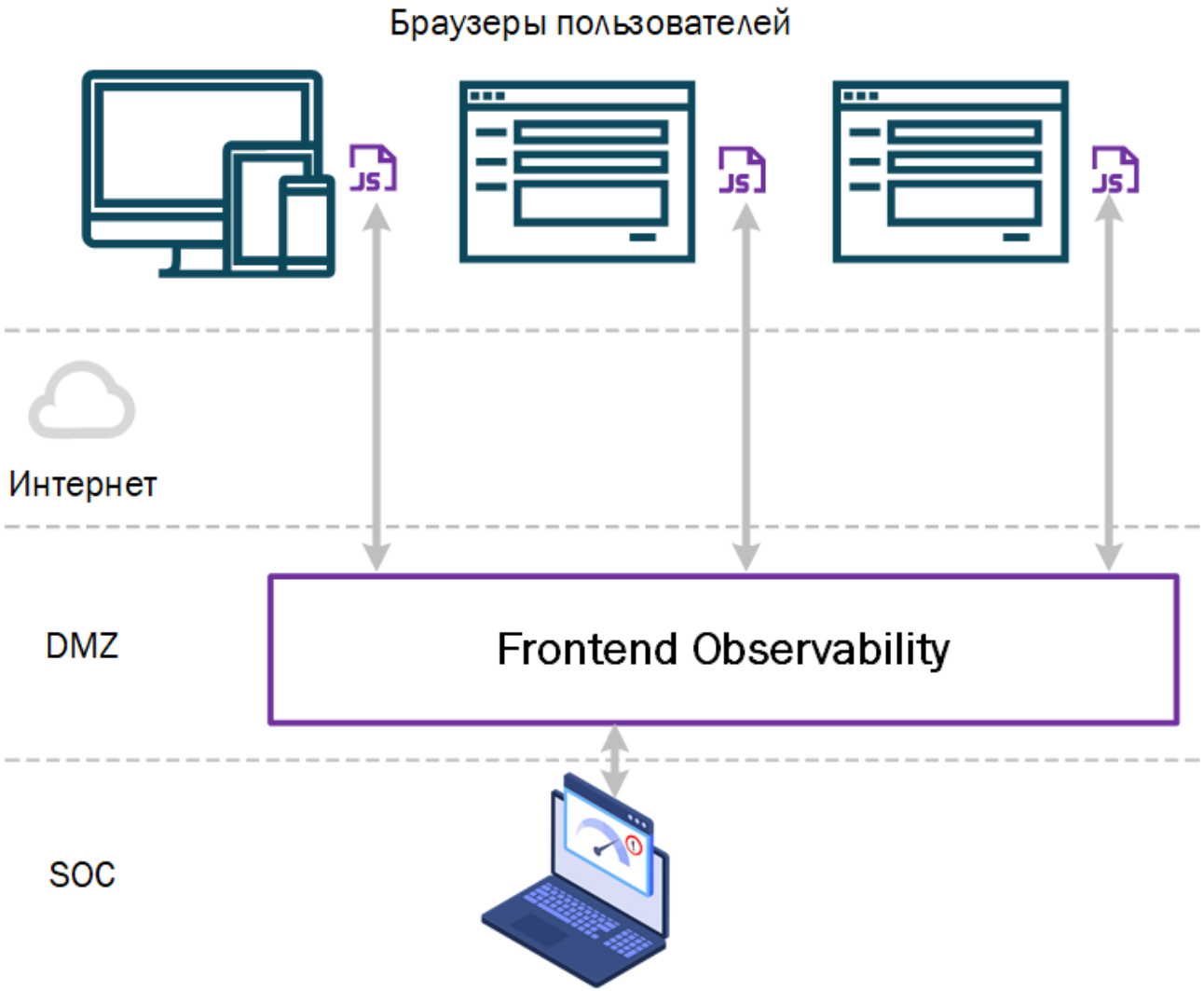
Software Bill of Behaviour (SBOB)

Контентный слой браузера

Frontend Observability

SOC FORUM 2024

- JS-агент, подключенный на страницы
- Инвентаризация скриптов и других активных элементов в реальном времени
- Мониторинг всех сетевых запросов js-приложения
- Выявления фактов появления на страницах конфиденциальных данных
- Применение правил корреляции
- Выявление критичных инцидентов
- Отправка событий в SIEM / SOC



Требования регуляторов

SOC FORUM 2024

НКЦКИ «Рекомендации по повышению уровня защищенности российских web-приложений» № ALRT-20220311.1 от 11 марта 2022 г.

19. **Перед использованием** на web-ресурсах JavaScript-кода, подгружаемого со сторонних ресурсов, **осуществлять его проверку на предмет вредоносного воздействия** на отображаемую в браузерах пользователя информацию и возможность кражи аутентификационных данных и файлов-cookie пользователей.

20. Осуществлять периодическую проверку хэш-сумм, используемых JavaScript. В случае изменения хэш-сумм отключать использование JavaScript на сайте и **выполнять повторную проверку функциональности**.

PCI DSS 4.0.1 (Требования вступают в силу 31.03.2025)

6.4.3 Все скрипты платежных страниц, которые загружаются и выполняются в браузере пользователя, управляются следующим образом:

- Реализован метод подтверждения **авторизации каждого скрипта**.
- Реализован метод, обеспечивающий **целостность каждого скрипта**.
- Актуальная **инвентаризация всех скриптов** с письменным обоснованием необходимости каждого из них.

11.6.1 Обнаружение и реагирование на несанкционированное изменение платежных страниц:

- Контроль **изменений на платежных страницах**
- Контроль **изменений HTTP-заголовков**
- Оповещение персонала о несанкционированных изменениях

Модель зрелости процесса мониторинга ИБ frontend-приложения

SOC FORUM 2024

- Базовый мониторинг сетевых запросов браузера через Content Security Policy (CSP) report-to (не все каналы)
- Периодическая инвентаризация всех скриптов

- Регулярный анализ приложения в frontend-sandbox (FAST-анализаторе), круглосуточно / каждый час. Эмулируются распространенные устройства пользователей.
  - Инвентаризация всех скриптов / активных элементов
  - Карта сетевых запросов
  - Используемые API-браузера
- Реагирование на любые отклонения от доверенной политики
- Особое внимание после новых релизов приложения

- Мониторинг поведения frontend-приложения в реальном времени:
  - Скрипты / активные элементы
  - Все сетевые запросы браузера
- Контроль объема / состава данных, передаваемых сторонним сервисам, контроль трансграничной передачи данных
- Выявление аномалий
- Реагирование на срабатывания правил корреляции (инциденты, затрагивающие значительное число пользователей)

Безопасное frontend-приложение

Что делать?

SOC FORUM 2024

- Ответить на вопрос: «Я знаю/уверен, что делает frontend-приложение прямо сейчас? Куда отправляет данные?»
- Использовать frontend-приложения в качестве источника событий для SOC
- Согласование с ИБ:
  - изменения js-кода;
  - новые хосты, с которыми взаимодействует js-приложение;
  - новые сторонние js-сервисы;
  - новые API-браузеры, используемые js-кодом.
- Использование встроенных механизмов безопасности браузера (CSP, SRI) для снижения базовых рисков

Telegram-канал FrontSecOps

SOC FORUM 2024

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

SOC FORUM 2024

@mkparfenov

Михаил Парфенов
DPA Analytics
https://dpa-analytics.ru/