



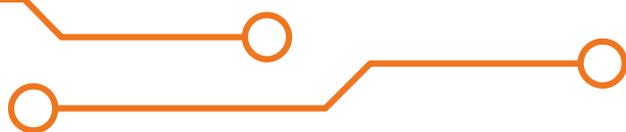
Вебмониторэкс

защита веб-приложений и API

API: от аудита к защите

Тимофей Горбунов

Сергей Одинцов



История компании

Основание
компании в РФ

2013


wallarm

Выход
на международный рынок

2016

Отделение российского бизнеса
в независимую компанию

2022

 **Вебмониторэкс**
защита веб-приложений и API

11 лет

Опыта разработки решений
по защите веб-приложений

>50%

R&D остались в России
в команде Вебмониторэкс

Вэбмониторэкс в 2025 году

80+

Технологических
интеграций

60+

Технических специалистов
среди сотрудников

200+

Реализованных проектов
в России

Топ-100

Крупнейших
ИБ-компаний в России



Технологическая база
международного уровня



Продукты в реестре
российского ПО



Техническая поддержка
24/7/365



Открытость и обратная
связь по всем продуктам

Технологический и инновационный лидер, ориентированный на практический результат

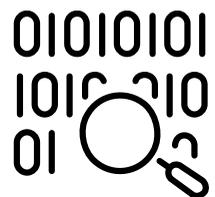
Платформа «Вебмониторэкс»

Защищает от атак на веб-приложения, микросервисы и API

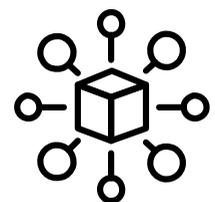
Продукт ПроWAF



Firewall
веб-приложений

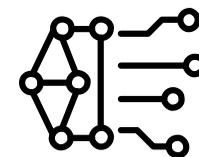


Сканер
периметра и уязвимостей

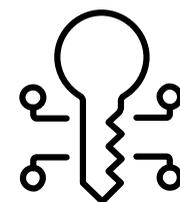


Модуль
перепроверки атак

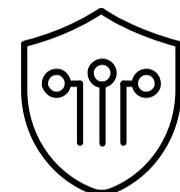
Линейка продуктов ПроAPI



ПроAPI Структура



ПроAPI Тестирование

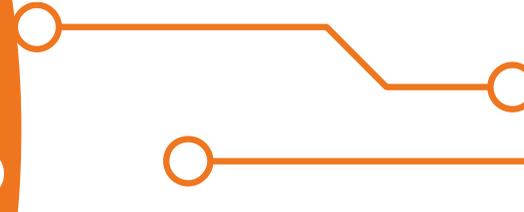


ПроAPI Защита



01

**Проблематика
в защите API**



Что обычно «смотрит наружу»



- Публичные веб-приложения
- Корпоративный сайт
- Внешние API

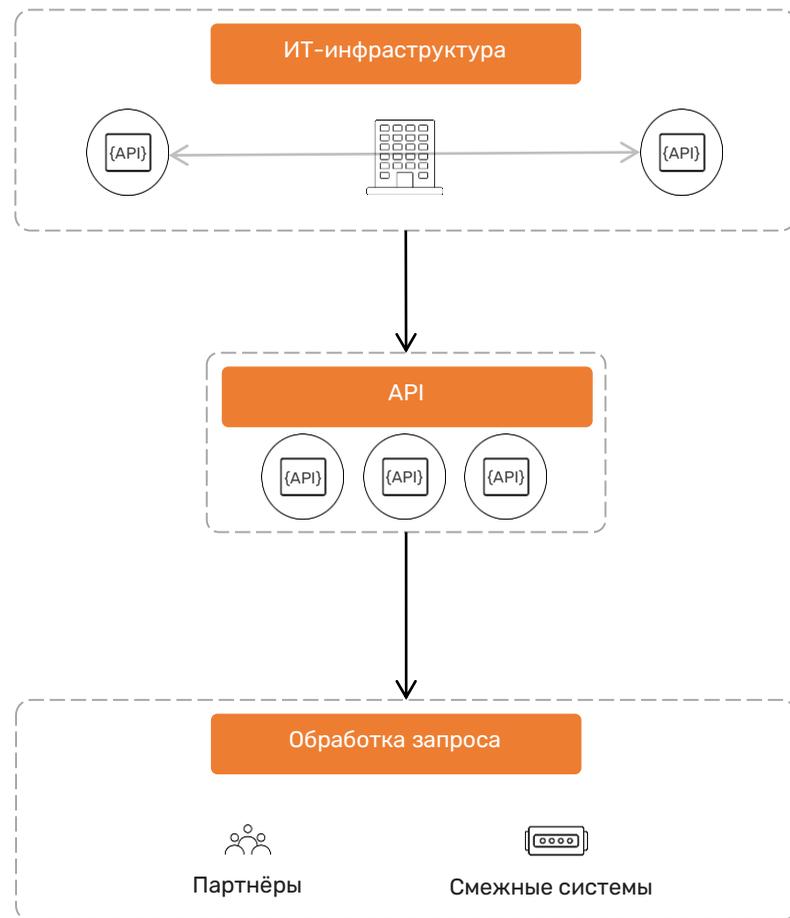
- Внутренние ресурсы для дочерних компаний и подрядчиков, выходящие за периметр
- Пользовательские и административные веб-интерфейсы business-critical систем
- **Неконтролируемое кросс-системное взаимодействие через API**

Как применяется

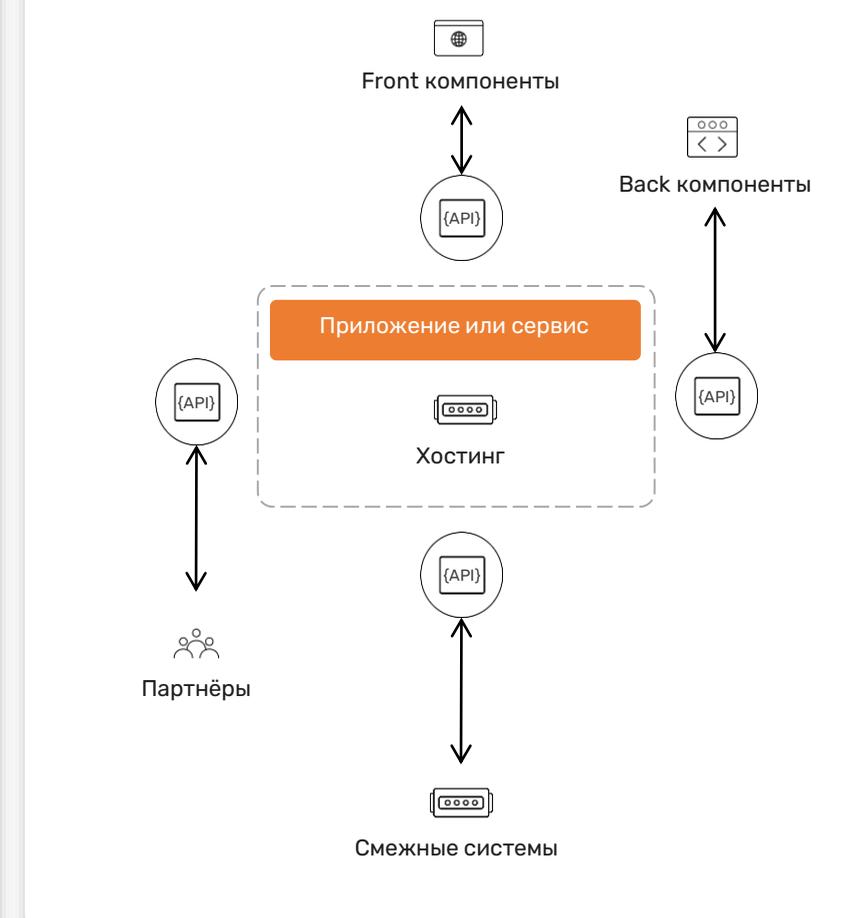
Для пользователя



Для компании



Для разработчика



Основные проблемы

Много доступных API

Много версий API с разными параметрами, нет понимания, какие точки несут наибольшую угрозу

Нет наблюдаемости

Непонятно что происходит с API, какие изменения, что происходит от момента дизайна до публикации

Нет инструмента автоматизации

Без требований к API не получается организовать процесс их контроля, при наличии требований – не получается автоматизировать

Основная угроза: доступность данных

Личных данных

Защита персональных, медицинских и банковских данных всегда находится в высоком приоритете, а их утечка ведет к значительным рискам

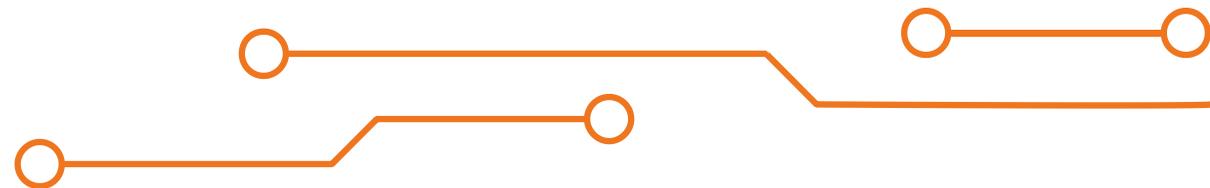
Бизнес-данных

Изменения в данных, на которых основывается бизнес – наиболее критичная угроза

Конфиденциальных данных

У каждой компании есть данные, раскрытие которых может привести к серьезным репутационным и финансовым потерям

Рост количества API



на 167%

увеличилось количество API
за последний год

66%

организаций управляют более чем 100 API
в 2024 году

в 5 раз

увеличилось количество эндпоинтов
по сравнению с началом 2023 года

59%

организаций управляют более чем 100 API
в 2023 году

Виды API:

- REST
- SOAP
- RPC
- Web Socket
- GraphQL

Рост атак на API

в 4 раза

увеличилось количество атак на веб-ресурсы российских компаний в 2024 году

Исследование ГК «Солар»

84%

организаций сообщили об инцидентах безопасности API за 2024

Исследование Akamai

Trello Breach (январь 2024)

Скомпрометированы данные более 15 миллионов пользователей

Dropbox API Keys Breach (май 2024)

Доступ к токенам аутентификации, данным многофакторной аутентификации, хешированным паролям и информации о клиентах

Dell API Breach (май 2024)

Доступ к portalу партнёров Dell и 49 миллионам записей клиентов

Cox Communications API Breach (июнь 2024)

Угроза миллионам модемов, позволяющая манипулировать конфигурациями сети

Что делать?

Инвентаризировать

Собирать полную картину: что, где, как и на каких технологиях работает

Документировать

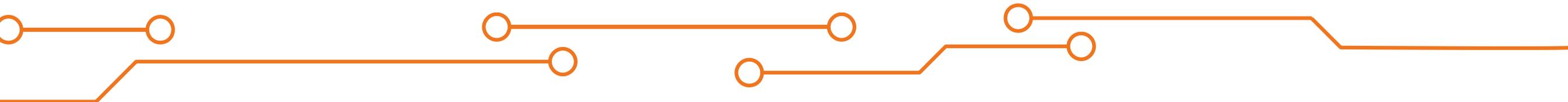
Создавать Open API Specification (OAS) – важнейший компонент, описывающий работу каждого API, который есть далеко не у всех компаний

Анализировать

Внедрять и использовать на этапе разработки code review, статические анализаторы, линтеры

Тестировать

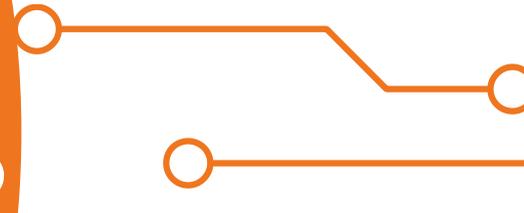
Автоматизировать тестирование, что позволит проводить его на регулярной основе и выявлять угрозы до релиза





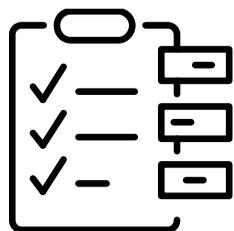
02

Подходы к защите API



Этапы реализации защиты API

Этап I: Знать



- Что есть в текущих API, из чего они состоят
- Какие данные передаются, какие точки используются
- Какие уязвимости и угрозы в API
- Когда происходит что-то anomalous на endpoint

Этап II: Защищать



- Контролировать расхождения с согласованной спецификацией (политикой)
- Заблокировать те endpoint, которые несут угрозу
- Автоматизировать реагирование при обнаружении угрозы (BOLA, обнаружение PII)

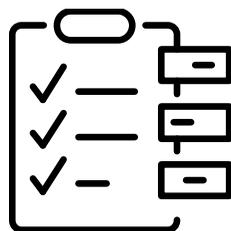
Этап III: Не допускать



- Фиксировать «нормальный» трафик запросов к API
- Блокировать все что не описано в OAS
- Блокировать все запросы с признаком утечки секретов
- Выявлять проблемные endpoint в API (Shadow API)

Результат каждого этапа

Этап I: Знать



- Сформулированы требования к командам разработки и инфраструктуры – политика управления API
- Инструмент отслеживания аномалий в API, первичный контроль цикла разработки
- Структурированная информация об уязвимостях и угрозах API

Этап II: Защищать



- Фиксация расхождений опубликованного и разрабатываемого API
- Автоматизация проверки требований политики API на стадии планирования, разработки и реализации API
- Блокировка эксплуатации уязвимостей до завершения исправлений приложения

Этап III: Не допускать

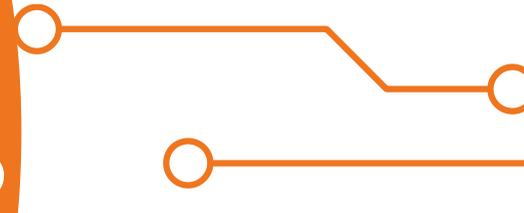


- Автоматическое соответствие политике управления API
- Полноценный контроль цикла разработки API
- Мониторинг всей цепочки передачи запросов приложений
- Полное доверие функционирующим процессам управления API



03

Компоненты линейки ПроAPI



API – это целый новый мир

ПроAPI Структура

Инвентаризация API, мониторинг изменений

- Визуализация структуры API
- Мониторинг изменений в структуре API
- Выявление наличия чувствительных данных
- Оценка рисков
- Экспорт построенной структуры в файл
- Валидация OAS
- Отслеживание атак на эндпоинты API (BOLA)

ПроAPI Тестирование

Заблаговременное выявление уязвимостей

- Проверка API по OAS
- Фаззинг эндпоинтов и параметров API
- Детектирование DoS-уязвимостей и аномалий
- Поиск инъекций
- Поиск уникальных уязвимостей API

ПроAPI Защита

Валидация трафика API в рамках OAS

- Усиление защиты REST и GraphQL API
- Предотвращение утечек данных
- Валидация JWT токенов
- Обнаружение Shadow API
- Блокировка запросов
- Централизованное управление

Описание процесса



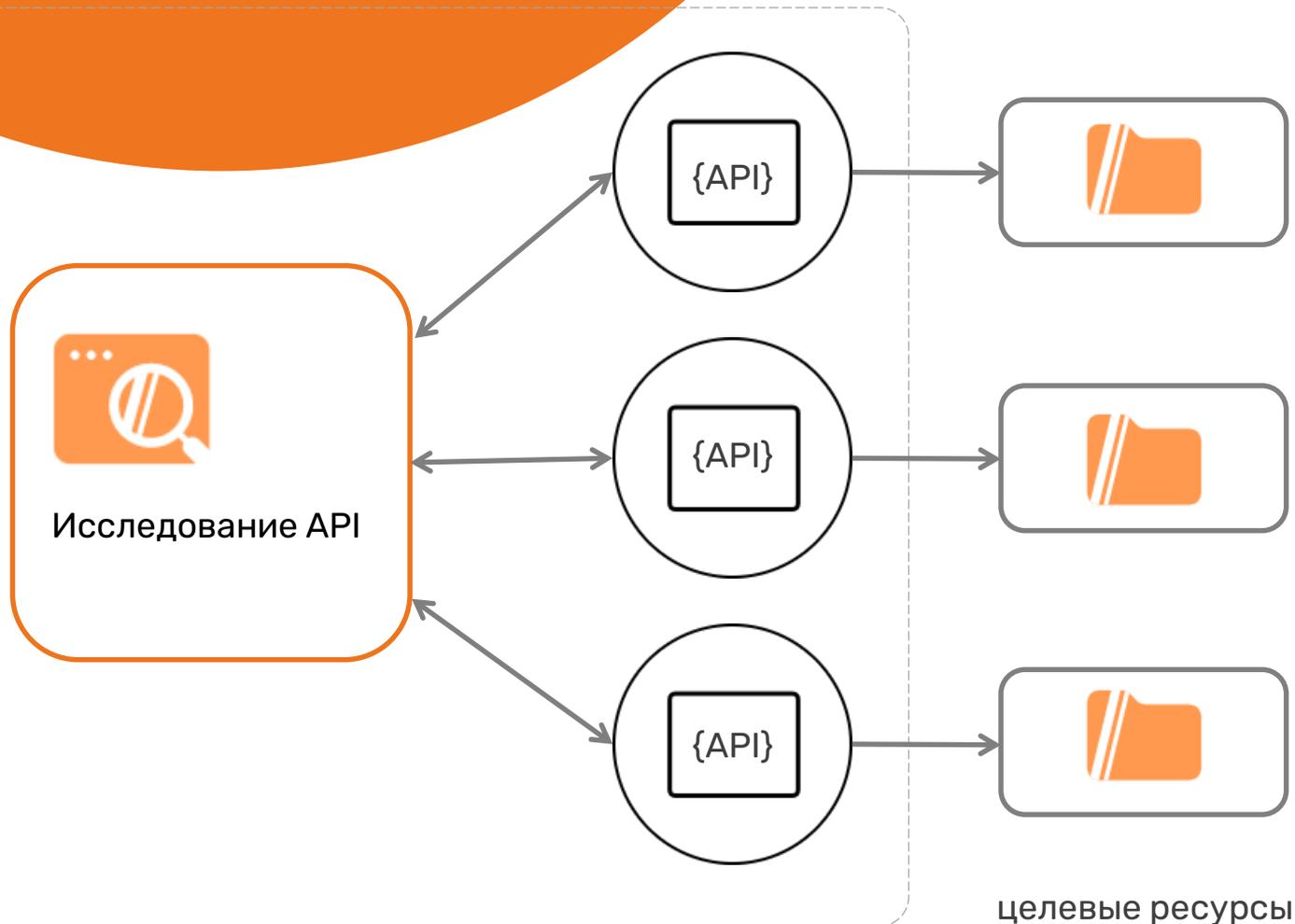
ПроAPI Структура (знать, защищать)



Модуль сбора OAS по трафику, предназначенный для обеспечения визуализации и анализа API, формирования политики API, блокирования наиболее критичных угроз API

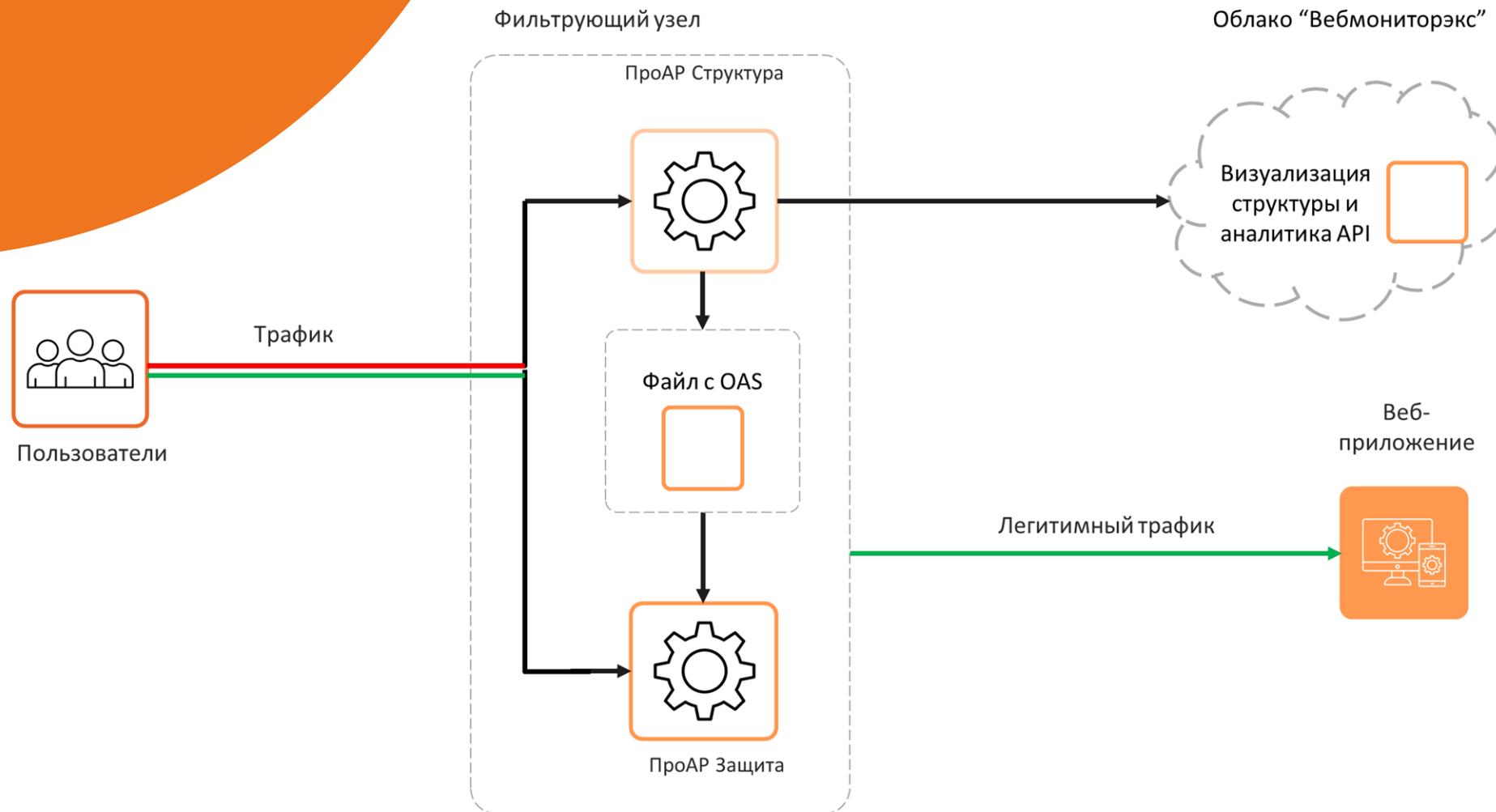
- Проверка реальной API по OAS, предоставленной командой разработки (выявить shadow и orphan API)
- Визуализация и анализ корректности построения API (на основе запросов к эндпоинтам и параметрам)
- Инструмент блокирования угроз и уязвимостей для эндпоинтов и маршрутов в API
- Выявление наличия чувствительных данных, передаваемых в эндпоинтах
- Расчет уровня риска для эндпоинтов

Продукт для инвентаризации API



- Механизм защиты API построен на основе **поведенческого ИИ**
- Технология быстро, точно и автоматически **подстраивается к изменяющимся параметрам API**, учитывая особенности каждой конкретной API и контекст ее работы.
- Независимо от того, где работают приложения, на каком технологическом стеке они основаны и сколько трафика потребляет ресурс, вы можете защитить **любые API веб-приложения или веб-сайты** от любых атак.

Схема установки



Функции продукта

- Ранжирование эндпоитов по риску
- Показ уязвимостей, ПДн
- Показ точек аутентификации
- Показ потенциальных точек для BOOLA
- Выгрузка спецификации или фрагмента
- Навигация по спецификации, именам параметров и типам передаваемых данных, типам содержимого

Планируется реализовать:

- Анализ ответов
- Сбор и отображение статистики по эндпоинтам
- Фиксирование и корректировка спецификации построенной на основе трафика

Структура API

Поиск по эндпоинтам

Main API ▾ main-api.ru.demo.webmonitorx.dev ▾ Метод ▾ PII ▾ Уровень риска ▾ Уязвимости ▾ Изменения в структуре API ▾ Изменения с 22 февр. 2024 ▾ Другие ▾

Хосты API

Все Публичные Внутренние

– Main API

- main-api.ru.demo.webmonito...

72 эндпоинта

Эндпоинт / Хост	Изменения	PII	Безопасность	Хиты	Риск
main-api.ru.demo.webmonitorx.dev					
<input type="button" value="GET"/> /about	<input type="button" value="Изменен"/>			12.5K	1.0
<input type="button" value="GET"/> /api/v1/admin/logs	<input type="button" value="Изменен"/>			14.3K	3.0
<input type="button" value="GET"/> /api/v1/admin/settings	<input type="button" value="Изменен"/>			252	1.0
<input type="button" value="PATCH"/> /api/v1/allocation/submission/{parameter_1}	<input type="button" value="Изменен"/>	<input type="button" value="👤"/>		11.4K	7.0
<input type="button" value="DELETE"/> /api/v1/allocation/submission/{parameter_1}	<input type="button" value="Изменен"/>			12.1K	5.0
<input type="button" value="GET"/> /api/v1/allocation/submission/{parameter_1}	<input type="button" value="Изменен"/>			5.28K	5.0
<input type="button" value="POST"/> /api/v1/allocation/submission/{parameter_1}	<input type="button" value="Изменен"/>	<input type="button" value="👤"/>		12.8K	7.0
<input type="button" value="PATCH"/> /api/v1/client/{parameter_1}	<input type="button" value="Изменен"/>	<input type="button" value="♂"/> <input type="button" value="\$"/> <input type="button" value="👤"/>		8.11K	8.0
<input type="button" value="POST"/> /api/v1/client/{parameter_1}	<input type="button" value="Изменен"/>	<input type="button" value="♂"/> <input type="button" value="\$"/> <input type="button" value="👤"/>		21.1K	8.0
<input type="button" value="DELETE"/> /api/v1/client/{parameter_1}	<input type="button" value="Изменен"/>			9.9K	5.0
<input type="button" value="GET"/> /api/v1/client/{parameter_1}	<input type="button" value="Изменен"/>			11K	5.0
<input type="button" value="GET"/> /api/v1/document	<input type="button" value="Изменен"/>			36.7K	1.0

ПроAPI Тестирование (знать, не допускать, защищать)

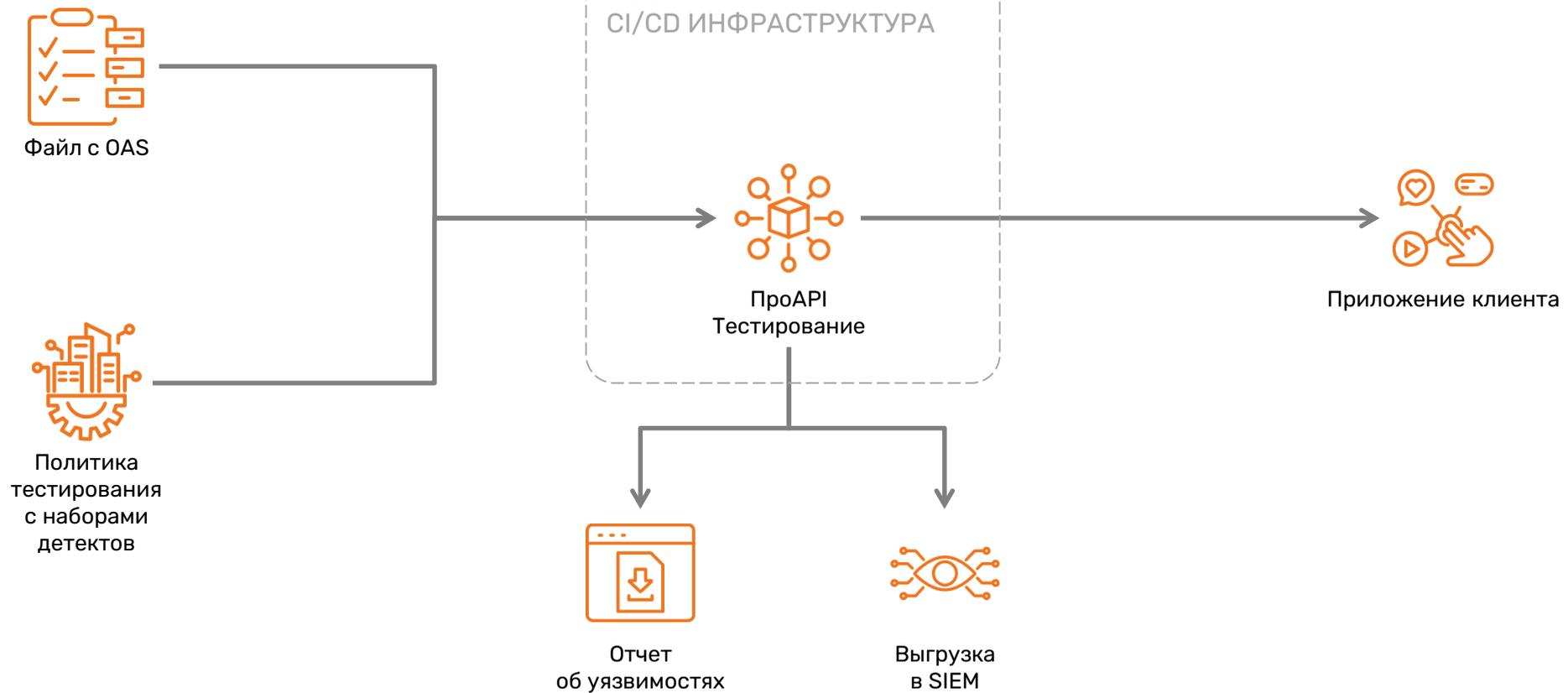


Инструмент для поиска ошибок, уязвимостей, включая 0-day уязвимости в веб-приложениях и API на основе OAS

- Проверка API по OAS, указанной вручную или полученной из ПроAPI «Структуры»
- Нативная интеграция в цикл разработки API, в CI/CD пайплайне
- Фаззинг эндпоинтов и параметров API для покрытия того, что не описано в OAS
- Поиск инъекций, покрытие OWASP TOP 10 & OWASP
- API TOP 10

Схема установки

ИНФРАСТРУКТУРА КЛИЕНТА





Тестирование API

Все спецификации

+ Создать тест

Политики

Все: 6

Активные: 4

Отключенные: 2

Тесты:	Статус	Спецификация	Количество тестируемых эндпоинтов		
Быстрая проверка целостности API Проверка конечных точек API на целостность данных и согласованность ответов.	В работе	APP-1	132/150	<input type="checkbox"/>	
Оценка эффективности конечной точки Оценка производительности конечной точки API и эффективности при различных нагрузках.	Запланирован 02.04.24	APP-1	102/100		
Проверка уровня владения протоколом Оценка соответствия протоколу API и совместимость на разных платформах.	Выключен	APP-1	99/120		
Набор стресс-тестов безопасности Оценка надежности безопасности API с помощью имитируемых атак и взлома данных.	Выключен	APP-1	13/15		
Проверка интерфейса взаимодействия Изучение совместимости API в различных системах и версиях.	Запланирован 12.04.24	загруженная спецификация	132/150		
Набор стресс-тестов безопасности Оценка надежности безопасности API с помощью имитируемых атак и взлома данных.	В работе	APP-2	12/90	<input type="checkbox"/>	

ПроAPI Защита (знать, не допускать, защищать)

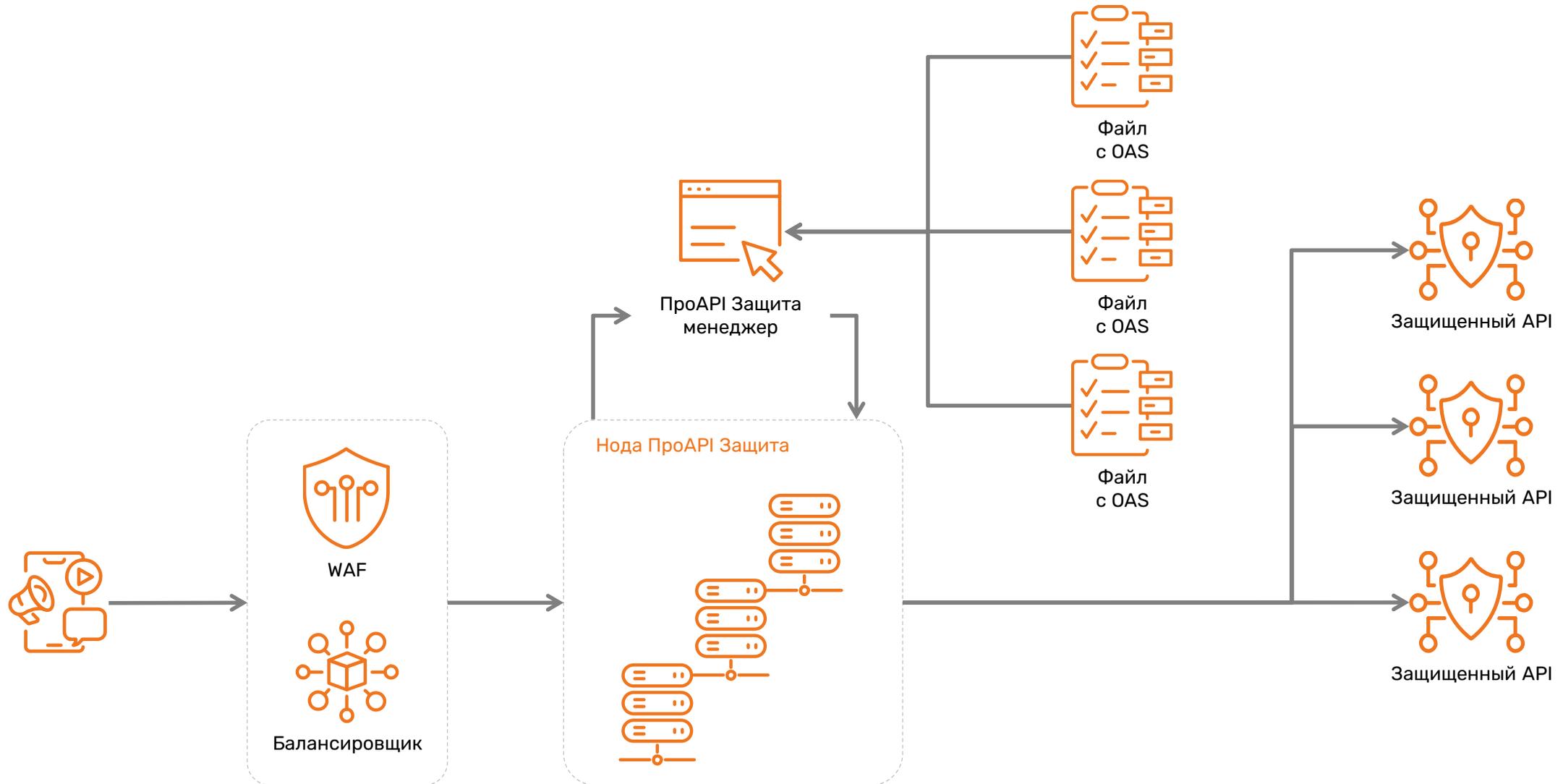


Инструмент для фиксации OAS и валидации запросов к API в рамках позитивной модели

Может быть использован, как локальный компонент, без подключения к облаку, так и с возможностью интеграции с облачным ЛК

- Усиление защиты REST API путем проверки запросов на соответствие заявленной спецификации OpenAPI 3.0 (позитивная модель)
- Предотвращение утечек данных путем проверки ответов приложения на соответствие заявленной спецификации
- Валидация JWT токенов в OAuth 2.0 аутентификации
- Обнаружение Shadow API – теневой версии API, которая может содержать устаревшие, небезопасные, незащищенные, развернутые для отладки методы и эндпоинты и может стать причиной утечек данных и компрометации системы
- Блокировка запросов с утекшими токенами, куками и прочим

Схема установки





- Дашборд
- События**
- Приложения
- Ноды
- Настройки

События

Поиск today ? Q

Выберите период ▼ Все события ▼ Метод ▼ Код ответа ▼ Все приложения ▼ 507 событий

Дата и время ▼	Тип	Топ IP/Источник	Метод	Домен и путь	Параметр	Код
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	POST	backend:4010 /parkedorders		403
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	POST	backend:4010 /salesoverview		403
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	POST	backend:4010 /vouchers/removereservation		403
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	POST	backend:4010 /qi/update		403

Node_ID: 67179a29868643d258ee2050
Request_ID: 93a3a632-7a32-4077-9079-b32bcb7ca164
Api_FW_version: omega
OAS_version: 1.0.0
Protocol: HTTP/1.1
Scheme: http

Message: request body has an error; doesn't match schema #/components/schemas/QuickItem: Error at "/dateofdelete": string doesn't match the format "date-time" (regular expression "[0-9]{4}-[0-9]{10}[112]-([0-9]{30}|31)T[0-9]{2}:[0-9]{2}(\.[0-9]+)?(Z|[+]{0-9}[2]:[0-9]{2})?S") Schema: {"description": "Note - Current format from database returns date and time as '2003-05-27T00:00:00.000+02:00' but only date is important. Timepart can be ignored", "example": "2022-05-27T14:31:27.158+02:00", "format": "date-time", "type": "string"} Value: "marquee+loop%3D1+width%3D0+onfinish%3Dpr%5Cu006fmp%28document.cookie%29%3EY000%3C%2Fmarquee%3E"

Parameter:

22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	
22 окт. 2024 15:30	Shadow API эндпоинт	172.26.0.9	
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	
22 окт. 2024 15:30	Ошибка валидации	172.26.0.9	

- 
- Дашборд
 - События
 - Приложения
 - Ноды
 - Настройки

Аналитика угроз ПроAPI Защита

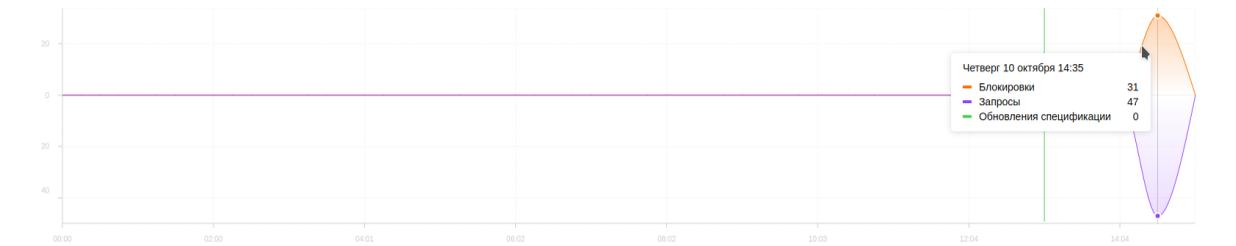
Easy_pos_app ▼

Сегодня ▼ Вчера ▼ Неделя ▼ Месяц ▼ 3 мес ▼ Год ▼ Выберите период ▼

Общие показатели

Запросов	Заблокированных запросов	Запросов в секунду	Обновлений спецификации
1 736	1 240	0	1

Запросы и блокировки



Четверг 10 октября 14:35

Заблокировки	31
Запросы	47
Обновления спецификации	0

— Заблокированные запросы — Запросы — Обновление спецификации

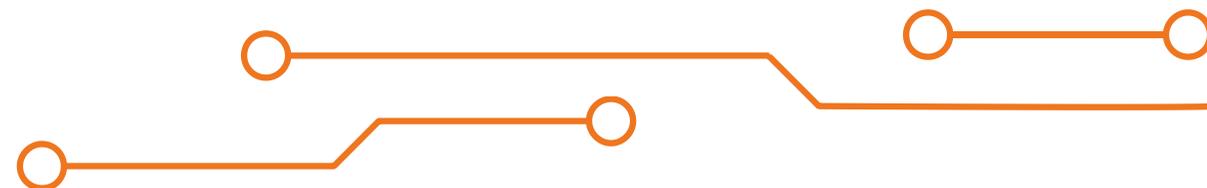
Карта покрытия по OWASP

Покрываем

- Broken Object Level Authorization
- Broken Authentication
- Unrestricted Resource Consumption
- Broken Function Level Authorization
- Unrestricted Access to Sensitive Business Flows
- Server Side Request Forgery
- Security Misconfiguration
- Improper Inventory Management

В разработке

- Broken Object Property Level Authorization
- Unsafe Consumption of APIs





04

**Кейсы
внедрения**



Пример проекта



Вебмониторэкс
защита веб-приложений и API

Задачи

Инфраструктура компании построена на основе микросервисов, взаимодействующих друг с другом по API, для которых необходимы учёт и мониторинг их изменений (5 веб-приложений, 3 мобильных приложения, 5 API, 1 интеграционный API)

Условия выбора продукта

- Совместимость с существующей инфраструктурой
- Использование в процессе безопасной разработки
- Техническая поддержка

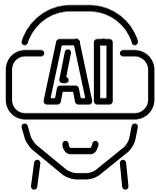
Результат

Внедрены продукты: ПроWAF, ПроAPI Структура, ПроAPI Тестирование и ПроAPI Защита

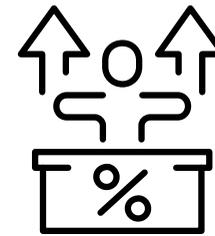
Преимущества платформы «Вебмониторэкс» для «СберАвто»

- Минимальное количество специалистов, необходимое для поддержки решений
- Минимальное время, затрачиваемое специалистами на поддержку решения (20%)
- Возможность обновления всех API раз в две недели
- Обеспечение безопасности веб-приложений и API
- Интеграция с другими процессами для обогащения
- Интеграция в процесс безопасной разработки
- Совместимость с облачной инфраструктурой
- Интеллектуальный подход
- Низкий уровень ложных срабатываний
- Поддержка процесса CI/CD

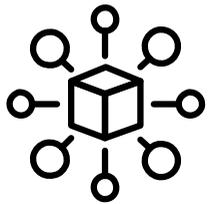
Присутствие в отраслях



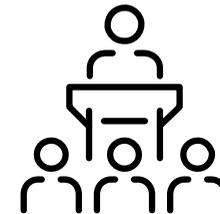
ИТ сектор



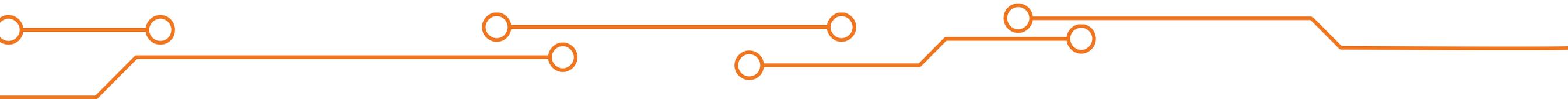
Финансовый сектор



E-commerce



Государственный сектор





Вебмониторэкс

защита веб-приложений и API



webmonitorx.ru



info@webmonitorx.ru



+7 495-740-35-44



[Habr](#)



[Телеграм](#)



[ВКонтакте](#)