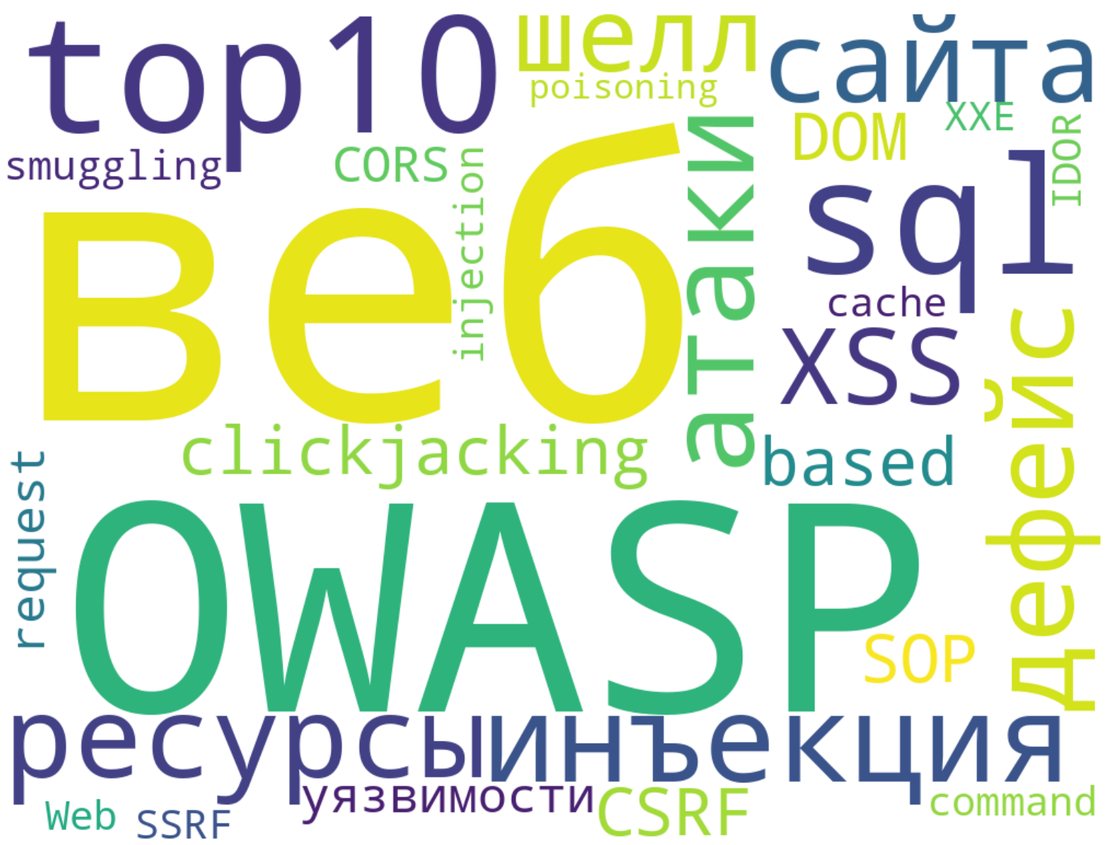
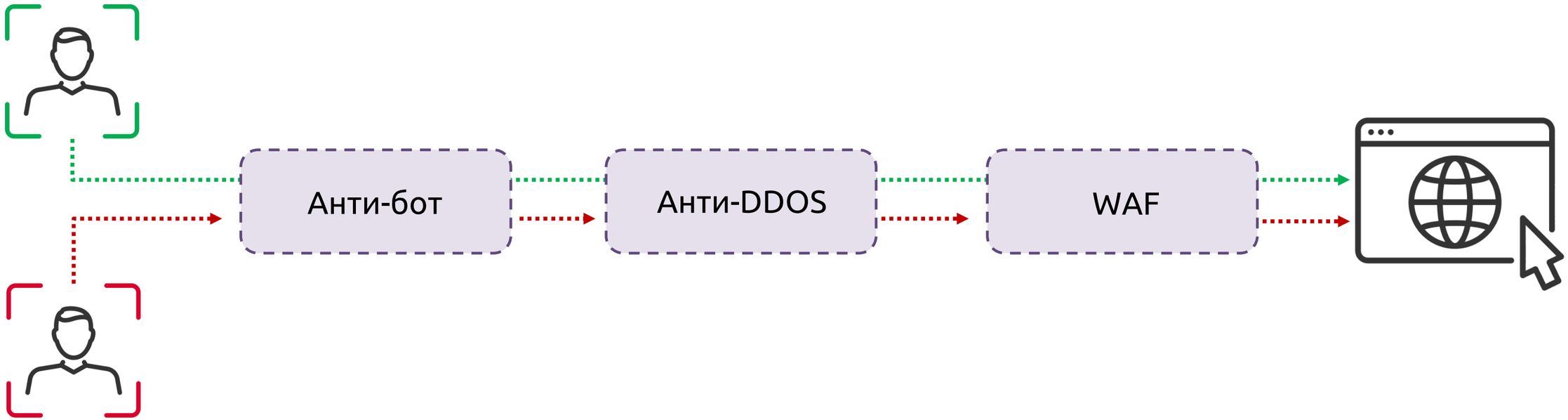
AML Web Protection – система выявления и предупреждения атак на веб-ресурсы

Александр Пушкин
Заместитель генерального директора
«Перспективный мониторинг»

Продукт решает классическую задачу



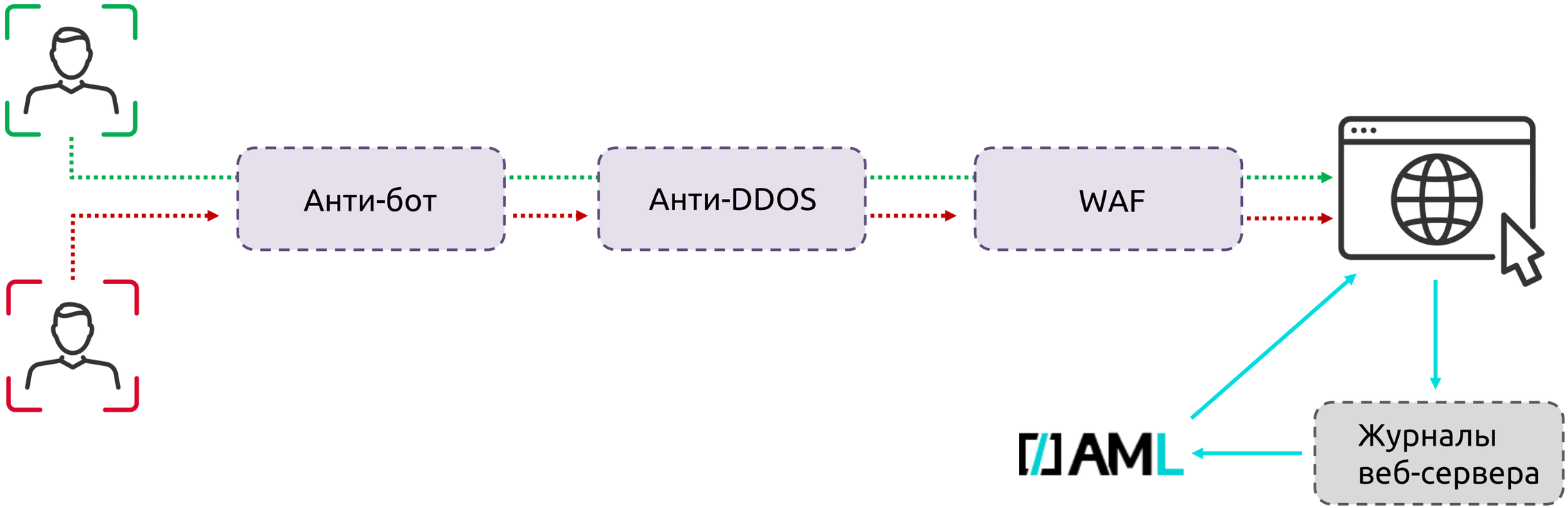
Текущая ситуация на рынке



- **Web Application Firewall (WAF)** – межсетевой экран уровня приложения

  Классическое СЗИ для защиты веб-приложений, API-интерфейсов
- **Анти-бот** – средство защиты от вредоносных ботов
- **Анти-DDoS** – средство защиты от атак на канал

Задача, как у WAF, но другим способом



Вопросы для размышления

1. Все ли веб-ресурсы на **внешнем периметре** защищены WAF?
2. Все ли критические бизнес-системы в **корпоративной сети** защищены WAF?
3. Сколько и какие атаки **пропускает** мой WAF?

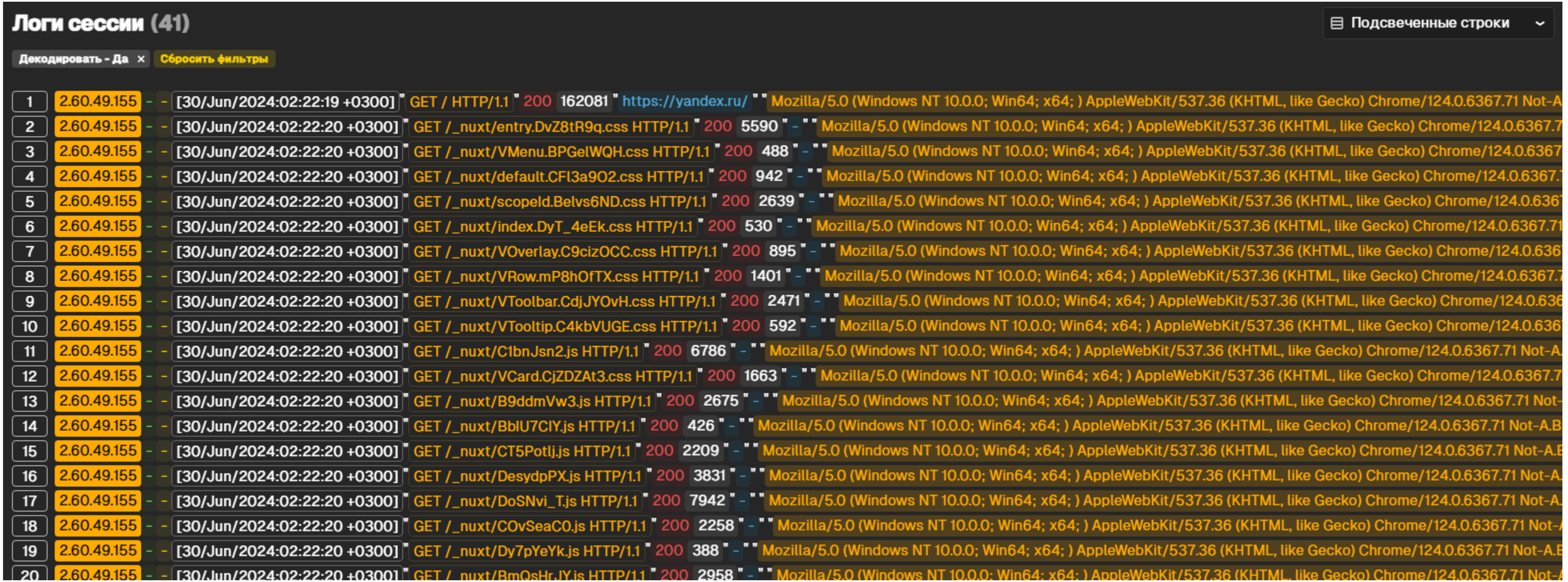
На вход подаются журналы веб-ресурсов

```
91.244.183.5 - - [30/Jul/2024:15:26:30 +0300] "GET /_nuxt/B28oeRTT.js HTTP/1.1" 200 48539 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:30 +0300] "GET /_nuxt/B7Utj78_.js HTTP/1.1" 200 63926 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:30 +0300] "GET /_nuxt/DzVWfiBp.js HTTP/1.1" 200 37199 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:30 +0300] "GET /_nuxt/BDQObz0O.js HTTP/1.1" 200 3398 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:30 +0300] "GET /_nuxt/CrETao-T.js HTTP/1.1" 200 20926 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:30 +0300] "GET /_nuxt/BIGtK6mf.js HTTP/1.1" 200 40386 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:31 +0300] "GET /_nuxt/nsV6cv1T.js HTTP/1.1" 200 285 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:31 +0300] "GET /_nuxt/BQ_rrzxf.js HTTP/1.1" 200 241 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:31 +0300] "GET /pattern.png HTTP/1.1" 200 1681 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
158.160.111.152 - - [30/Jul/2024:15:26:35 +0300] "GET / HTTP/1.1" 200 161407 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
10.10.4.254 - - [30/Jul/2024:15:26:35 +0300] "GET / HTTP/1.1" 200 161386 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
91.244.183.5 - - [30/Jul/2024:15:26:35 +0300] "GET / HTTP/1.1" 200 161102 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:35 +0300] "GET /_nuxt/default.CFl3a9O2.css HTTP/1.1" 200 942 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:35 +0300] "GET /_nuxt/entry.DvZ8tR9q.css HTTP/1.1" 200 5590 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:35 +0300] "GET /_nuxt/scopeId.Belvs6ND.css HTTP/1.1" 200 2639 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
91.244.183.5 - - [30/Jul/2024:15:26:36 +0300] "GET /api/v1/flags/status HTTP/1.1" 200 846 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0"
158.160.111.152 - - [30/Jul/2024:15:27:05 +0300] "GET / HTTP/1.1" 200 161395 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
10.10.4.254 - - [30/Jul/2024:15:27:05 +0300] "GET / HTTP/1.1" 200 161412 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
10.10.4.254 - zbx_monitor [30/Jul/2024:15:27:14 +0300] "GET /api/overview HTTP/1.1" 400 248 "-" "-"
10.10.4.254 - zbx_monitor [30/Jul/2024:15:27:15 +0300] "GET /api/nodes/rabbit?memory=true HTTP/1.1" 400 248 "-" "-"
10.10.4.254 - zbx_monitor [30/Jul/2024:15:27:16 +0300] "GET /api/queues HTTP/1.1" 400 248 "-" "-"
158.160.111.152 - - [30/Jul/2024:15:27:35 +0300] "GET / HTTP/1.1" 200 161387 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
10.10.4.254 - - [30/Jul/2024:15:27:35 +0300] "GET / HTTP/1.1" 200 161404 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
158.160.111.152 - - [30/Jul/2024:15:28:04 +0300] "GET / HTTP/1.1" 200 161384 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
10.10.4.254 - - [30/Jul/2024:15:28:05 +0300] "GET / HTTP/1.1" 200 161398 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
10.10.4.254 - zbx_monitor [30/Jul/2024:15:28:14 +0300] "GET /api/overview HTTP/1.1" 400 248 "-" "-"
10.10.4.254 - zbx_monitor [30/Jul/2024:15:28:15 +0300] "GET /api/nodes/rabbit?memory=true HTTP/1.1" 400 248 "-" "-"
10.10.4.254 - zbx_monitor [30/Jul/2024:15:28:16 +0300] "GET /api/queues HTTP/1.1" 400 248 "-" "-"
158.160.111.152 - - [30/Jul/2024:15:28:34 +0300] "GET / HTTP/1.1" 200 161394 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
10.10.4.254 - - [30/Jul/2024:15:28:35 +0300] "GET / HTTP/1.1" 200 161395 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
158.160.111.152 - - [30/Jul/2024:15:29:04 +0300] "GET / HTTP/1.1" 200 161408 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
10.10.4.254 - - [30/Jul/2024:15:29:05 +0300] "GET / HTTP/1.1" 200 161409 "-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987.132 Safari/537.36"
```

На выходе — атакующие и пользовательские сессии

Дата и время начала	IP адрес	Риск 1	User-Agent	Количество строк	Предсказание подтверждено
01.07.2024 16...	34.143.170.145	Низкий риск	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom...	20	Да | Нет
04.07.2024 0...	51.77.53.200	Низкий риск	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom...	18	Да | Нет
05.07.2024 1...	92.223.85.66	Низкий риск	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom...	19	Да | Нет
12.07.2024 12...	92.223.85.73	Низкий риск	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom...	19	Да | Нет
30.06.2024 0...	158.160.111.152	Риск отсутств...	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.398...	240	Да | Нет
30.06.2024 0...	10.10.4.254	Риск отсутств...	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.398...	241	Да | Нет
30.06.2024 0...	80.251.239.97	Риск отсутств...	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64;) AppleWebKit/537.36 (KHTML, like Gecko) Chr...	190	Да | Нет
30.06.2024 0...	2.60.49.155	Риск отсутств...	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64;) AppleWebKit/537.36 (KHTML, like Gecko) Chr...	41	Да | Нет
30.06.2024 0...	158.160.111.152	Риск отсутств...	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.398...	241	Да | Нет

Как AML это делает?



Как AML это делает?

AML может работать с любыми веб-ресурсами и НЕ требует времени на обучение

Основные возможности

- **Выявление** атакующих сессий на веб-ресурсы
- **Блокировка** атакующих сессий
- **Пакетная** обработка журналов веб-серверов
- **Потоковая** обработка журналов
- Непрерывное **обучение**
- Выявление атак **нулевого** дня
- **Не зависит от стека** защищаемого веб-ресурса
- Поддержка **виртуального патчинга**

Сравнение WAF и AML

Функциональная характеристика	WAF	AML Web Protection
Принцип детектирования атаки	На базе отдельных запросов (сигнатурный анализ)	На базе сессий (группа запросов, объединенных по критериям. Поведенческий анализ)
Архитектура подключения	Устанавливается в «разрыв» (перед веб-ресурсом, может быть точкой отказа)	Устанавливается «сбоку» (получает журналы с веб-сервера)
Анализ зашифрованного трафика	Да (требует значительных аппаратных ресурсов)	Анализ записей журнала (не трафика
Блокировка вредоносного трафика	Да	Да (с помощью механизмов веб-сервера или других МСЭ)

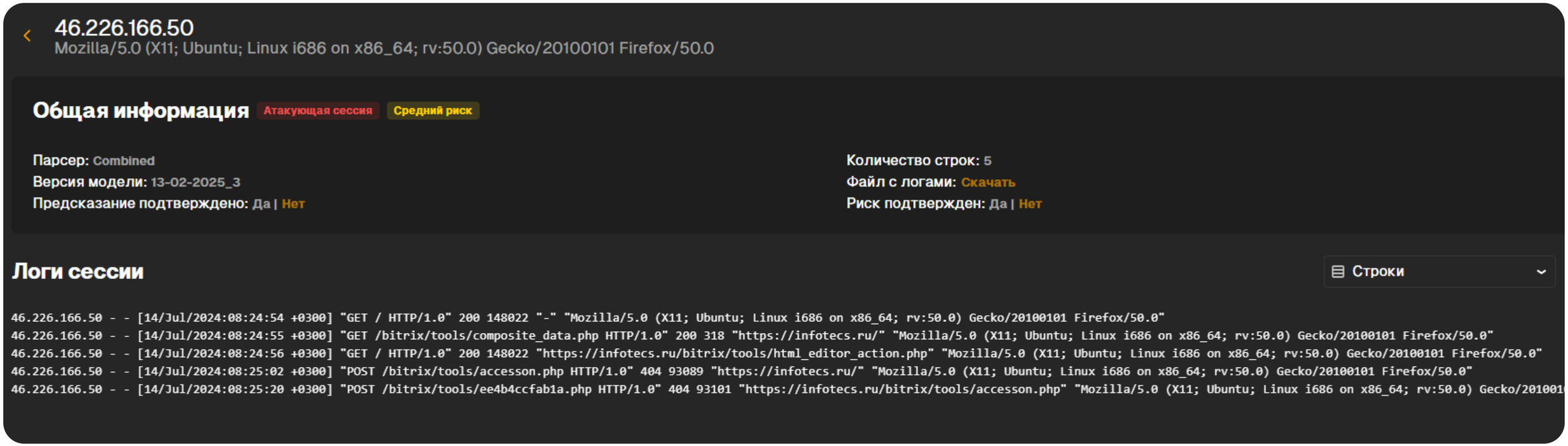
Сравнение WAF и AML

Функциональная характеристика	WAF	AML Web Protection
Внедрение	Сложно (стоимость внедрения иногда может достигать стоимости WAF)	Просто (требуется настройка передачи журналов встроенными средствами)
Размещение веб-ресурса для защиты	Внешний периметр, облако	Внешний периметр, облако, внутренние сайты
Ретроспективный анализ (анализ событий из прошлого)	Частично	Да (передача журнала веб-сервера)
Скорость блокировки	До передачи запроса на веб-сервер	После передачи журнала (не более 1 мин, что позволяет заблокировать атаку до наступления ущерба)

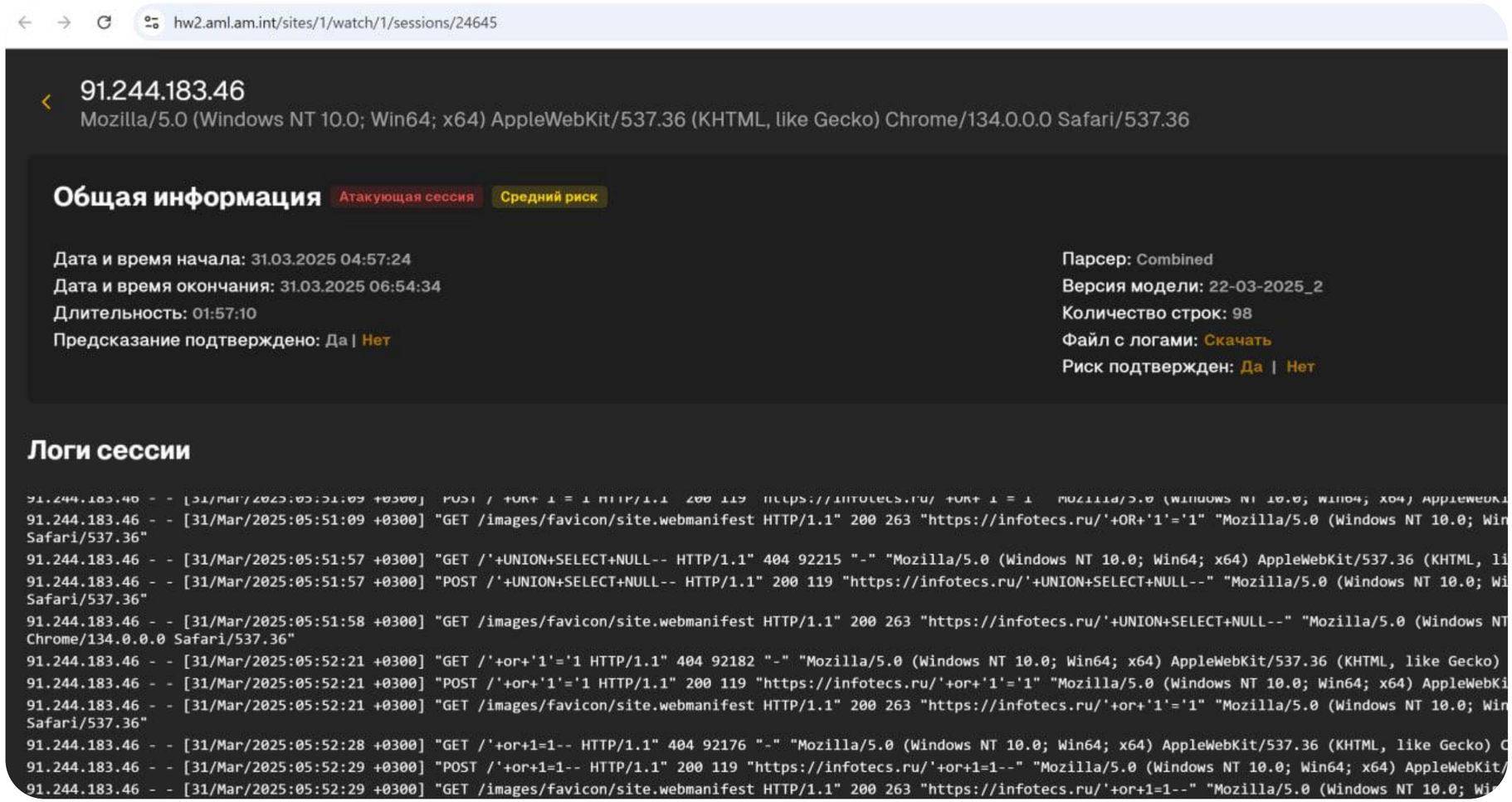
Показатели работы AML

Веб-ресурс	Режим	Сессий всего	Подтверждено атак	Допущено ошибок	% ошибок	Сторонние СЗИ
Сайт Министерства цифрового развития и связи субъекта РФ	потоковый, 15 дней 24/7	3 606	10	4 ложных срабатывания	0,1	WAF
Сайт Администрации Правительства субъекта РФ	потоковый, 15 дней 24/7	20 037	12	7 ложных срабатываний	0,03	WAF
Информационный портал образования субъекта РФ	пакетный, весь 2024 год	1 429 661	43	39 - ложных срабатываний 18 - пропусков (однотипные атаки)	0,004	WAF

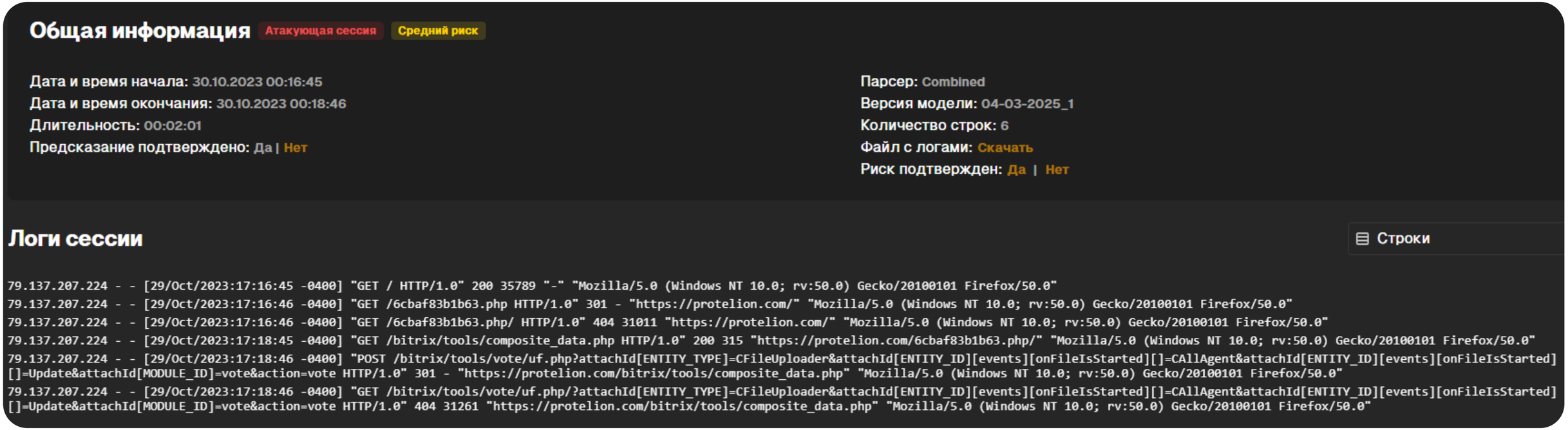
Угнать за 26 сек.



UNION + SELECT



Старый добрый vote



Общая информация Атакующая сессия Средний риск

Дата и время начала: 30.10.2023 00:16:45
Дата и время окончания: 30.10.2023 00:18:46
Длительность: 00:02:01
Предсказание подтверждено: Да | Нет

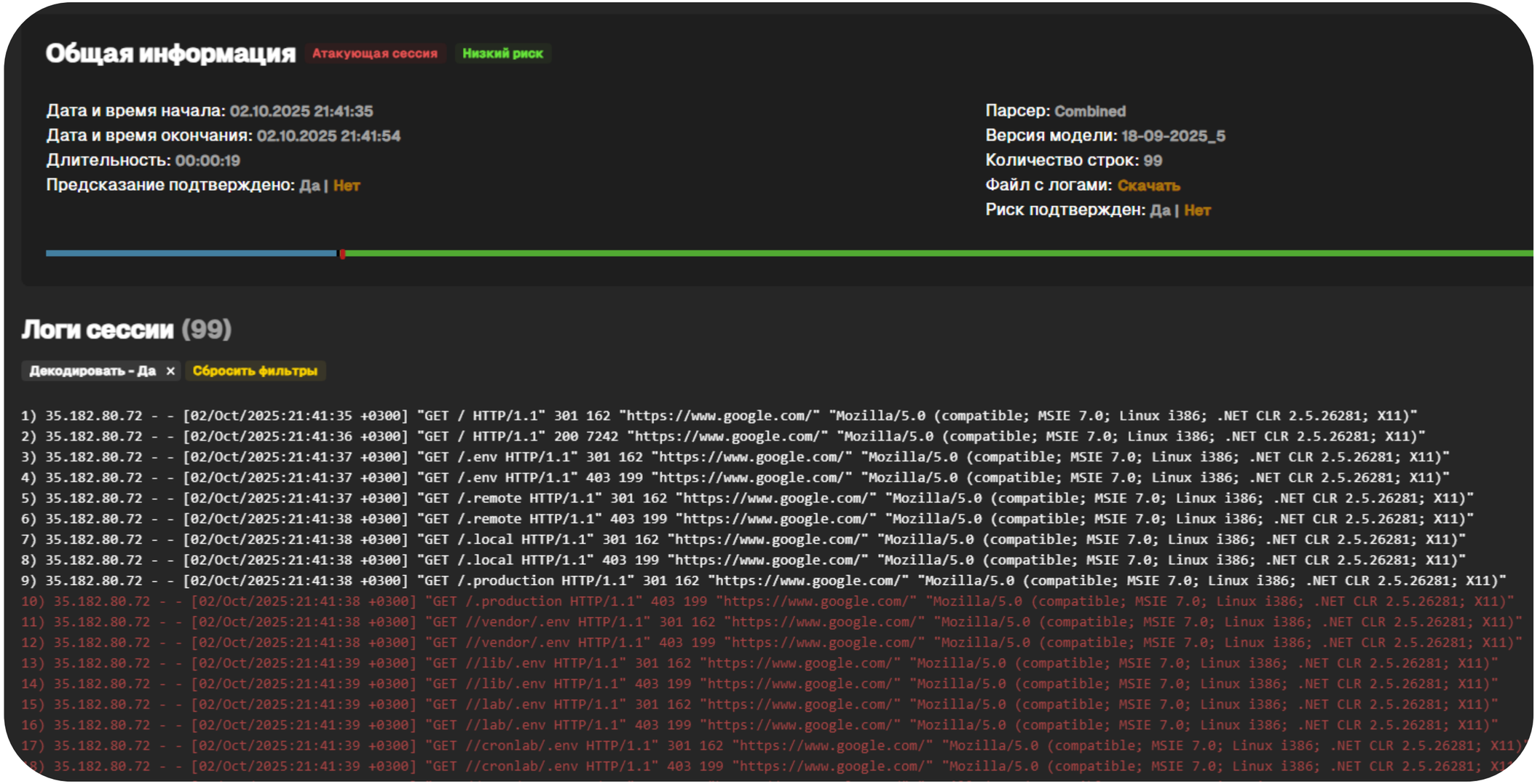
Парсер: Combined
Версия модели: 04-03-2025_1
Количество строк: 6
Файл с логами: Скачать
Риск подтвержден: Да | Нет

Логи сессии

Строки

```
79.137.207.224 - - [29/Oct/2023:17:16:45 -0400] "GET / HTTP/1.0" 200 35789 "-" "Mozilla/5.0 (Windows NT 10.0; rv:50.0) Gecko/20100101 Firefox/50.0"
79.137.207.224 - - [29/Oct/2023:17:16:46 -0400] "GET /6cbaf83b1b63.php HTTP/1.0" 301 - "https://protelion.com/" "Mozilla/5.0 (Windows NT 10.0; rv:50.0) Gecko/20100101 Firefox/50.0"
79.137.207.224 - - [29/Oct/2023:17:16:46 -0400] "GET /6cbaf83b1b63.php/ HTTP/1.0" 404 31011 "https://protelion.com/" "Mozilla/5.0 (Windows NT 10.0; rv:50.0) Gecko/20100101 Firefox/50.0"
79.137.207.224 - - [29/Oct/2023:17:18:45 -0400] "GET /bitrix/tools/composite_data.php HTTP/1.0" 200 315 "https://protelion.com/6cbaf83b1b63.php/" "Mozilla/5.0 (Windows NT 10.0; rv:50.0) Gecko/20100101 Firefox/50.0"
79.137.207.224 - - [29/Oct/2023:17:18:46 -0400] "POST /bitrix/tools/vote/uf.php?attachId[ENTITY_TYPE]=CFileUploader&attachId[ENTITY_ID][events][onFileIsStarted][]=CAllAgent&attachId[ENTITY_ID][events][onFileIsStarted]
[]=Update&attachId[MODULE_ID]=vote&action=vote HTTP/1.0" 301 - "https://protelion.com/bitrix/tools/composite_data.php" "Mozilla/5.0 (Windows NT 10.0; rv:50.0) Gecko/20100101 Firefox/50.0"
79.137.207.224 - - [29/Oct/2023:17:18:46 -0400] "GET /bitrix/tools/vote/uf.php/?attachId[ENTITY_TYPE]=CFileUploader&attachId[ENTITY_ID][events][onFileIsStarted][]=CAllAgent&attachId[ENTITY_ID][events][onFileIsStarted]
[]=Update&attachId[MODULE_ID]=vote&action=vote HTTP/1.0" 404 31261 "https://protelion.com/bitrix/tools/composite_data.php" "Mozilla/5.0 (Windows NT 10.0; rv:50.0) Gecko/20100101 Firefox/50.0"
```

3 секунды


Общая информация
Атакующая сессия
Низкий риск
Дата и время начала: 02.10.2025 21:41:35
Дата и время окончания: 02.10.2025 21:41:54
Длительность: 00:00:19
Предсказание подтверждено: Да | Нет
Парсер: Combined
Версия модели: 18-09-2025_5
Количество строк: 99
Файл с логами: Скачать
Риск подтвержден: Да | Нет
Логи сессии (99)
Декодировать - Да
Сбросить фильтры
1) 35.182.80.72 - - [02/Oct/2025:21:41:35 +0300] "GET / HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
2) 35.182.80.72 - - [02/Oct/2025:21:41:36 +0300] "GET / HTTP/1.1" 200 7242 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
3) 35.182.80.72 - - [02/Oct/2025:21:41:37 +0300] "GET /.env HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
4) 35.182.80.72 - - [02/Oct/2025:21:41:37 +0300] "GET /.env HTTP/1.1" 403 199 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
5) 35.182.80.72 - - [02/Oct/2025:21:41:37 +0300] "GET /.remote HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
6) 35.182.80.72 - - [02/Oct/2025:21:41:38 +0300] "GET /.remote HTTP/1.1" 403 199 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
7) 35.182.80.72 - - [02/Oct/2025:21:41:38 +0300] "GET /.local HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
8) 35.182.80.72 - - [02/Oct/2025:21:41:38 +0300] "GET /.local HTTP/1.1" 403 199 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
9) 35.182.80.72 - - [02/Oct/2025:21:41:38 +0300] "GET /.production HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
10) 35.182.80.72 - - [02/Oct/2025:21:41:38 +0300] "GET /.production HTTP/1.1" 403 199 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
11) 35.182.80.72 - - [02/Oct/2025:21:41:38 +0300] "GET //vendor/.env HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
12) 35.182.80.72 - - [02/Oct/2025:21:41:38 +0300] "GET //vendor/.env HTTP/1.1" 403 199 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
13) 35.182.80.72 - - [02/Oct/2025:21:41:39 +0300] "GET //lib/.env HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
14) 35.182.80.72 - - [02/Oct/2025:21:41:39 +0300] "GET //lib/.env HTTP/1.1" 403 199 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
15) 35.182.80.72 - - [02/Oct/2025:21:41:39 +0300] "GET //lab/.env HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
16) 35.182.80.72 - - [02/Oct/2025:21:41:39 +0300] "GET //lab/.env HTTP/1.1" 403 199 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
17) 35.182.80.72 - - [02/Oct/2025:21:41:39 +0300] "GET //cronlab/.env HTTP/1.1" 301 162 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"
18) 35.182.80.72 - - [02/Oct/2025:21:41:39 +0300] "GET //cronlab/.env HTTP/1.1" 403 199 "https://www.google.com/" "Mozilla/5.0 (compatible; MSIE 7.0; Linux i386; .NET CLR 2.5.26281; X11)"

ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

AML Web Protection

Спасибо
за внимание!

Александр Пушкин,

заместитель генерального директора,
«Перспективный мониторинг»

Aleksandr.Pushkin@amonitoring.ru

t.me/pm_public

amonitoring.ru

ТЕХНО infotecs ФЕСТ

Подписывайтесь
на наши соцсети,
там много интересного

CYBER MEDIA

NBJ НАЦИОНАЛЬНЫЙ БАНКОВСКИЙ ЖУРНАЛ

GLOBAL DIGITAL SPACE

CISOCLUB

РУТОКЕН КОМПАНИЯ АКТИВ

ПЕРСПЕКТИВНЫЙ МОНИТОРИНГ

АВАНГАРД

ARinteg

АТБ ЭЛЕКТРОНИКА

infotecs {/-cademy}

merlion

УЧЕБНЫЙ ЦЕНТР ИНФОТЕКС