

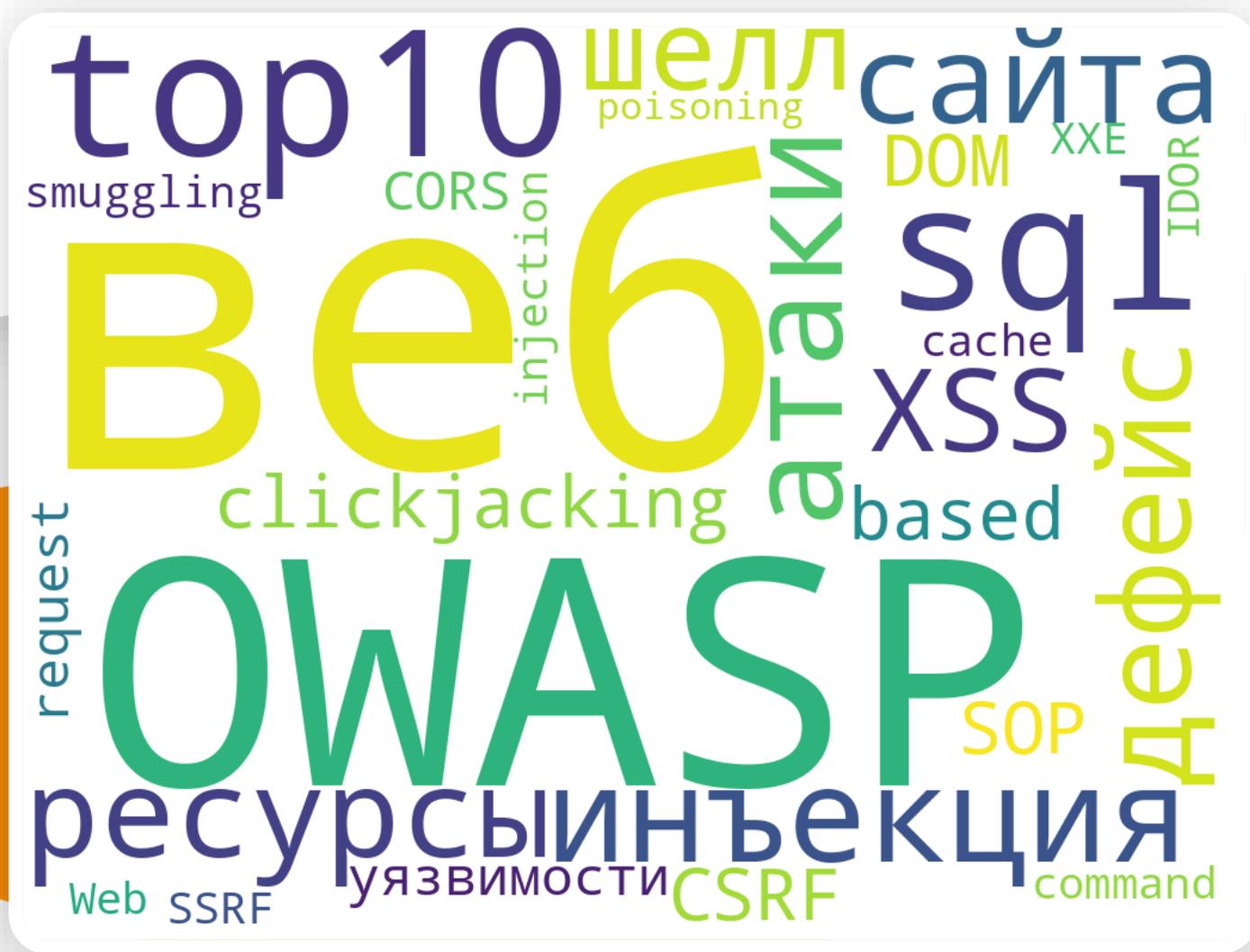
# AML Web Protection — система выявления и предупреждения атак на веб-ресурсы

Александр Пушкин,  
Заместитель генерального директора,  
«Перспективный мониторинг»

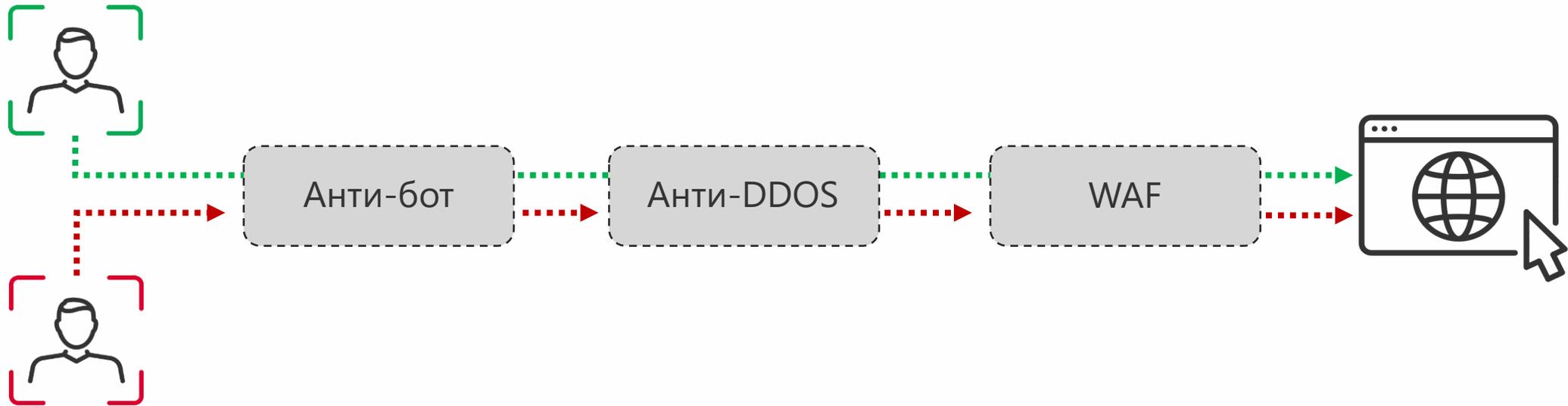


**AML**

Продукт решает классическую задачу

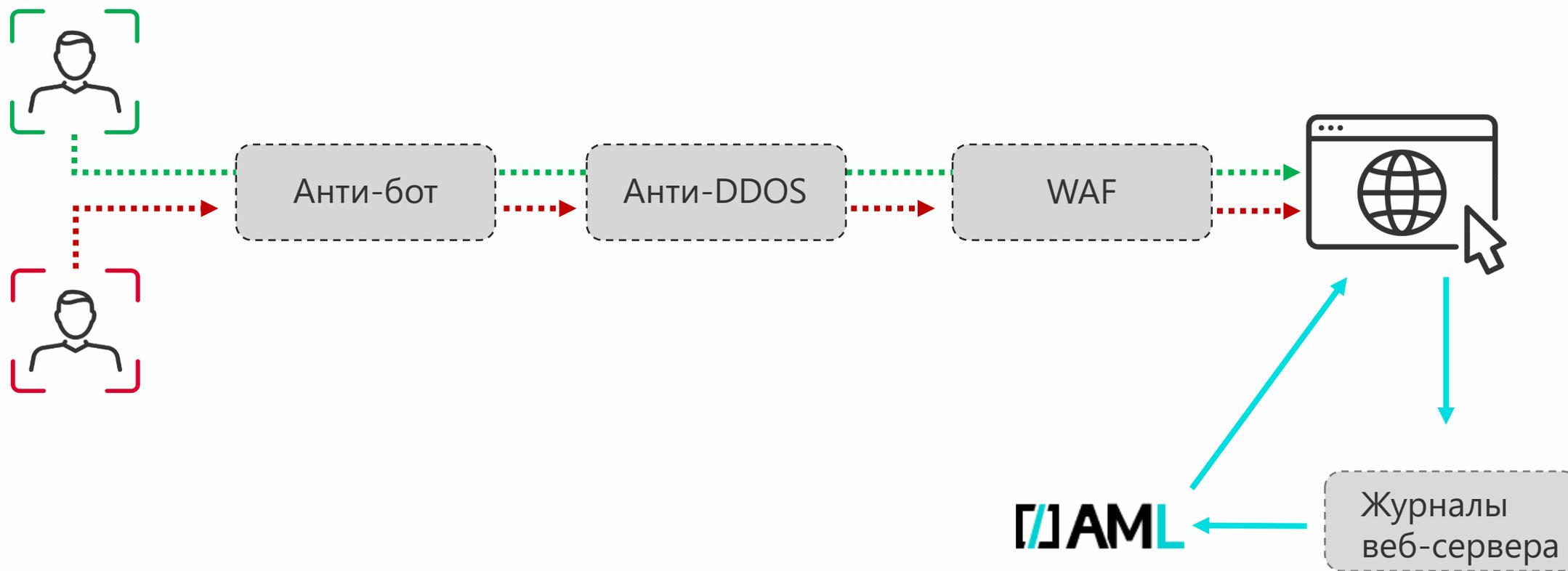


# Текущая ситуация на рынке



- 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/DzVWfipP.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/nsV6cviT.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



IP адрес ↕	Риск ↕ 1	User-Agent ↕	Количество строк ↕	Риск подтвержден	Предсказание подтверждено	⚙️
👤 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	Да   Нет	
👤 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	Да   Нет	
👤 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	Да   Нет	
👤 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	Да   Нет	
👤 158.160.111.152	Риск отсутств...	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987....	240	-	Да   Нет	
👤 10.10.4.254	Риск отсутств...	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/80.0.3987....	241	-	Да   Нет	
👤 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	
👤 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	

# Как AML это делает?



Логи сессии (41) Подсвеченные строки

Декодировать - Да Сбросить фильтры

1	2.60.49.155	-	[30/Jun/2024:02:22:19 +0300]	GET / HTTP/1.1	200	162081	"https://yandex.ru/"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-A
2	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/entry.DvZ8tR9q.css HTTP/1.1	200	5590	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.7
3	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/VMenu.BPGelWQH.css HTTP/1.1	200	488	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367
4	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/default.CF13a9O2.css HTTP/1.1	200	942	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367
5	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/scopeld.Belvs6ND.css HTTP/1.1	200	2639	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.636
6	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/index.DyT_4eEk.css HTTP/1.1	200	530	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.7
7	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/VOverlay.C9cizOCC.css HTTP/1.1	200	895	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.636
8	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/VRow.mP8hOfTX.css HTTP/1.1	200	1401	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.7
9	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/VToolbar.CdjJYOvH.css HTTP/1.1	200	2471	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.636
10	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/VTooltip.C4kbVUGE.css HTTP/1.1	200	592	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.636
11	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/C1bnJsn2.js HTTP/1.1	200	6786	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-A
12	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/VCard.CjZDZAt3.css HTTP/1.1	200	1663	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.7
13	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/B9ddmVw3.js HTTP/1.1	200	2675	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-
14	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/BblU7CIY.js HTTP/1.1	200	426	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-A.B
15	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/CT5Potlj.js HTTP/1.1	200	2209	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-A.E
16	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/DesydpPX.js HTTP/1.1	200	3831	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-A
17	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/DoSNvi_T.js HTTP/1.1	200	7942	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-A
18	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/COvSeaCO.js HTTP/1.1	200	2258	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-
19	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/Dy7pYeYk.js HTTP/1.1	200	388	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-A.E
20	2.60.49.155	-	[30/Jun/2024:02:22:20 +0300]	GET /_nuxt/BmQsHr_IV.js HTTP/1.1	200	2958	"	Mozilla/5.0 (Windows NT 10.0.0; Win64; x64; ) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.6367.71 Not-



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**

**WJAML**

# Текущая ситуация на рынке



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)

# Текущая ситуация на рынке



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	поточковый, 30 дней 24/7	8 316	98	4 ложных срабатывания	0,05	WAF
Сайт Администрации Правительства субъекта РФ	поточковый, 30 дней 24/7	39 037	51	7 ложных срабатываний	0,04	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.



**46.226.166.50**  
Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86\_64; rv:50.0) Gecko/20100101 Firefox/50.0

**Общая информация** Атакующая сессия Средний риск

Парсер: Combined  
Версия модели: 13-02-2025\_3  
Предсказание подтверждено: Да | Нет

Количество строк: 5  
Файл с логами: [Скачать](#)  
Риск подтвержден: Да | Нет

**Логи сессии** Строки

```
46.226.166.50 - - [14/Jul/2024:08:24:54 +0300] "GET / HTTP/1.0" 200 148022 "-" "Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64; rv:50.0) Gecko/20100101 Firefox/50.0"
46.226.166.50 - - [14/Jul/2024:08:24:55 +0300] "GET /bitrix/tools/composite_data.php HTTP/1.0" 200 318 "https://infotecs.ru/" "Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64; rv:50.0) Gecko/20100101 Firefox/50.0"
46.226.166.50 - - [14/Jul/2024:08:24:56 +0300] "GET / HTTP/1.0" 200 148022 "https://infotecs.ru/bitrix/tools/html_editor_action.php" "Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64; rv:50.0) Gecko/20100101 Firefox/50.0"
46.226.166.50 - - [14/Jul/2024:08:25:02 +0300] "POST /bitrix/tools/accession.php HTTP/1.0" 404 93089 "https://infotecs.ru/" "Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64; rv:50.0) Gecko/20100101 Firefox/50.0"
46.226.166.50 - - [14/Jul/2024:08:25:20 +0300] "POST /bitrix/tools/ee4b4ccfab1a.php HTTP/1.0" 404 93101 "https://infotecs.ru/bitrix/tools/accession.php" "Mozilla/5.0 (X11; Ubuntu; Linux i686 on x86_64; rv:50.0) Gecko/20100101 Firefox/50.0"
```

# UNION+SELECT



← → ↻ 📄 hw2.aml.am.int/sites/1/watch/1/sessions/24645

< 91.244.183.46  
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36

### Общая информация

Атакующая сессия Средний риск

Дата и время начала: 31.03.2025 04:57:24	Парсер: Combined
Дата и время окончания: 31.03.2025 06:54:34	Версия модели: 22-03-2025_2
Длительность: 01:57:10	Количество строк: 98
Предсказание подтверждено: Да   Нет	Файл с логами: <a href="#">Скачать</a>
	Риск подтвержден: Да   Нет

### Логи сессии

```
91.244.183.46 - - [31/Mar/2025:05:51:09 +0300] POST /+or+1=1 HTTP/1.1 200 119 "https://infotecs.ru/+or+1=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:51:09 +0300] "GET /images/favicon/site.webmanifest HTTP/1.1" 200 263 "https://infotecs.ru/'+or+1'=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:51:57 +0300] "GET /'+UNION+SELECT+NULL-- HTTP/1.1" 404 92215 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:51:57 +0300] "POST /'+UNION+SELECT+NULL-- HTTP/1.1" 200 119 "https://infotecs.ru/'+UNION+SELECT+NULL--" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:51:58 +0300] "GET /images/favicon/site.webmanifest HTTP/1.1" 200 263 "https://infotecs.ru/'+UNION+SELECT+NULL--" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:52:21 +0300] "GET /'+or+1'=1 HTTP/1.1" 404 92182 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:52:21 +0300] "POST /'+or+1'=1 HTTP/1.1" 200 119 "https://infotecs.ru/'+or+1'=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:52:21 +0300] "GET /images/favicon/site.webmanifest HTTP/1.1" 200 263 "https://infotecs.ru/'+or+1'=1" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:52:28 +0300] "GET /'+or+1=1-- HTTP/1.1" 404 92176 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:52:29 +0300] "POST /'+or+1=1-- HTTP/1.1" 200 119 "https://infotecs.ru/'+or+1=1--" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
91.244.183.46 - - [31/Mar/2025:05:52:29 +0300] "GET /images/favicon/site.webmanifest HTTP/1.1" 200 263 "https://infotecs.ru/'+or+1=1--" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36"
```

# 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)"
```

# Параметры лицензирования AML [//]



Веб-ресурс	Lite	Business	Enterprise
Суммарный EPS в секунду	0-50 EPS	50-200 EPS	200-500 EPS

# Принципы пилотирования AML



- **Минимальная нагрузка** на технических специалистов заказчика
- **Исключение** негативного влияния на инфраструктуру
- Два варианта пилотирования: пакетный и потоковый режим
- AML как проверка эффективности WAF

 AML

# Пакетный режим



Что на вход	Результат
<p>Журналы <b>access.log</b> веб-сервера(-ов) за любой период для 1-3 сайтов</p>	<ol style="list-style-type: none"><li>1. Результирующий pdf-отчет с показателями выявленных атак</li><li>2. Архив с набором атакующих сессий</li></ol>

# Потоковый режим



Что на вход	Результат
<ol style="list-style-type: none"><li>1. Установка ПО AML Web Protection на сервер заказчика или мы привозим готовый ПАК</li><li>2. Синхронизация журналов веб-сервера с AML</li><li>3. Обучение специалистов заказчика работе с AML (1-2 часа)</li></ol>	<ol style="list-style-type: none"><li>1. Мониторинг атак в реальном времени</li><li>2. Ретроспективный анализ</li><li>3. Подготовка результирующих отчетов</li><li>4. Блокировка атак (по желанию)</li></ol>



[amonitoring.ru](http://amonitoring.ru)



[t.me/pm\\_public](https://t.me/pm_public)

# Спасибо за внимание!

Александр Пушкин,  
заместитель генерального директора,  
«Перспективный мониторинг»

[Aleksandr.Pushkin@amonitoring.ru](mailto:Aleksandr.Pushkin@amonitoring.ru)