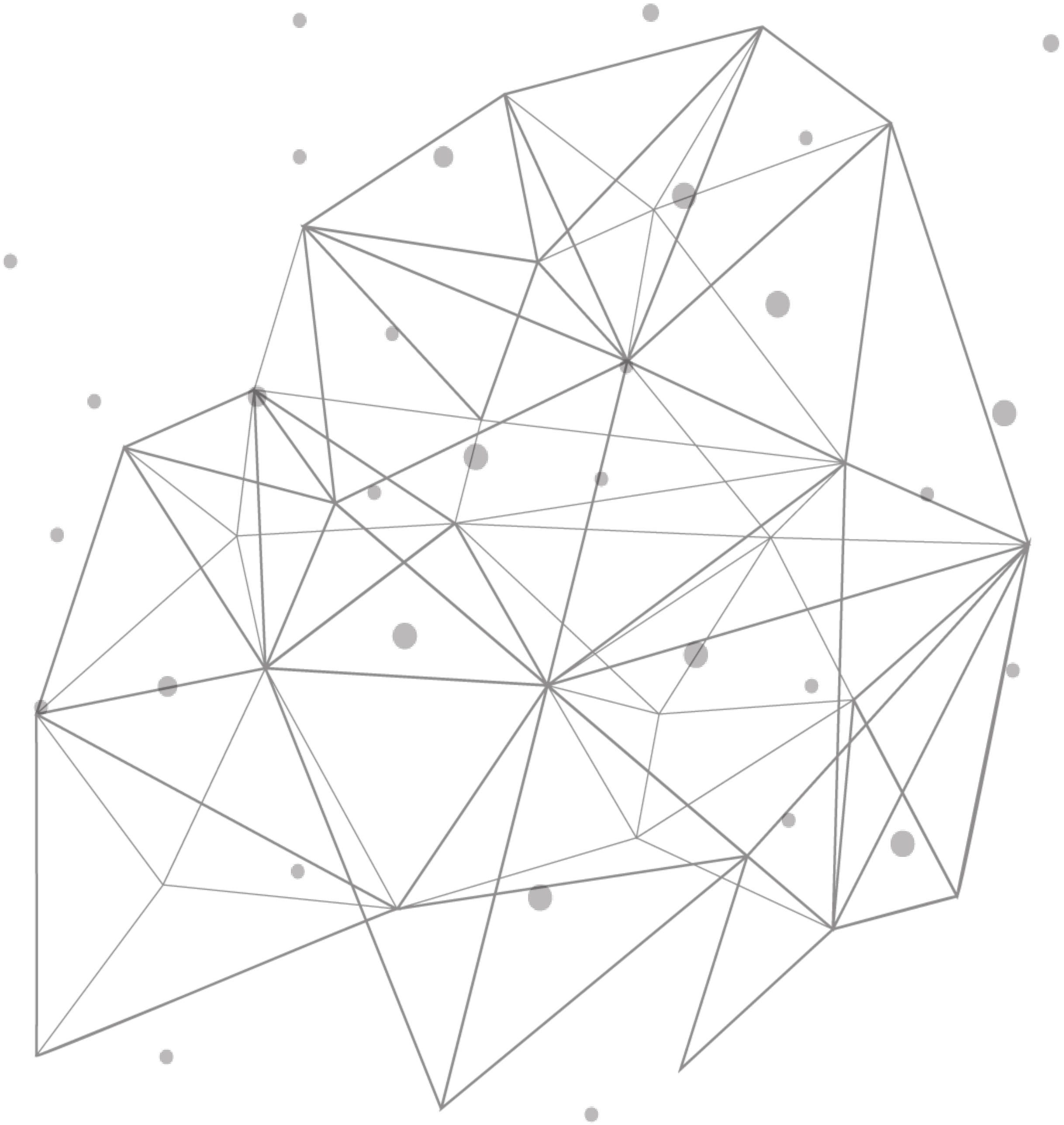
DOMAIN GENERATION ALGORITHMS



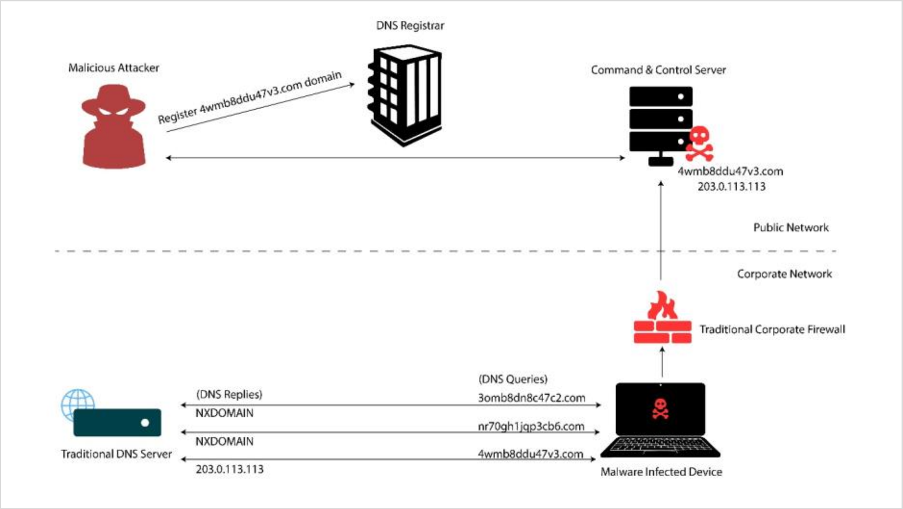
Introduction

TCPWave's flexible and extensive DNS TITAN platform offers superior protection & performance. Powered by machine learning and artificial intelligence. The advanced threat intelligence features that are embedded into the Network Security Management (NSM) models of the TCPWave IPAM have been widely acclaimed by many existing customers. The threat intelligence of TCPWave, along with the comprehensive features does not require any separate license to realize the benefits. The DNS TITAN, powered with a performance-tuned Atlantis Deep Learning model is a part of the base license of the TCPWave DDI offering.

Domain Generation Algorithms

Domain Generation Algorithms (DGA) is a technique used by malicious attackers to bypass traditional security mechanisms such as blacklisting of domains, reverse engineering malware to detect hardcoded Command and Control server's IP addresses and domain names.

With DGA attackers can generate a huge amount of random domain names which the malware attempts to connect using DNS queries. With a shared seed and DGA between the malware and the attacker, the attacker registers one of the generated domains to resolve the Command and Control (C&C) server. The malware tries to resolve the generated domains until it discovers the Command-and-Control server and starts communicating with it. This technique of random generation and disposal of registered domains, also known as Domain-Fluxing or Fast-Flux, makes it difficult for the security teams to blacklist domains and takedown the C&C server.



There are about 56 known DGA families according to Netlab. Some of them include gameover, cryptolocker, abcbot, Mirai, etc. The classification is based on the parameters like generated pattern length, characters used, notation, etc. of the domains. Some examples are mentioned below:

DGA Family	Example
Cryptolocker	nvjwoofansjbh.ru
Gameover	14dtuor1aubbmjhgup7915tlinc.net
Abcbot	knjpeuzyr.tk
Mirai	xvrvdsuhphjg.tech

Having DGA infected malware devices inside the network poses the risk of data exfiltration using DNS tunnels. Detection methodologies like log analysis of the suspicious DNS traffic are not only laborious and time-consuming but are also prone to evaluation errors.

TCPWave Titan

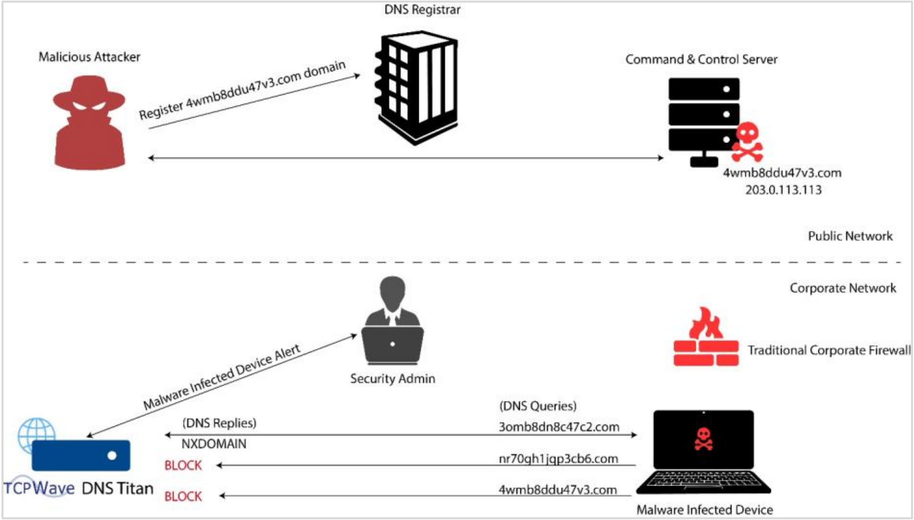
DNS TITAN is one of the solutions that TCPWave provides to combat the DGAs, which detects the traffic, alerts security engineers, and blocks malicious IP. DNS TITAN uses In-House built tunnel detection Machine Learning (ML) algorithms are trained using massive and varied DNS data thereby helping it to learn and detect the malicious DNS traffic flowing through the DNS pathways in your organization.

Machine Learning techniques are broadly categorized into Supervised, Unsupervised, and Reinforcement learning based on the signal or feedback available to train the models. Supervised learning is machine learning, in which machines are trained on labeled Data. Unsupervised learning uses ML algorithms to analyze the patterns and clusters in the Data. And Reinforcement learning trains the sequence of actions to maximize the reward.

The TCPWave Threat Intelligence leverages Supervised Machine Learning techniques like Decision Tree (DT), Random Forest (RF) Support Vector Machine (SVM) and K-Nearest Neighbors (KNN), also Deep Learning techniques like Convolution Neural Networks (CNN), Long- and Short-Term Memory (LSTM) Networks and Artificial Neural Networks (ANN) to detect malicious traffic flowing on DNS.

The TCPWave has trained and validated the models combining more than one technique along with one technique at a time, to add an extra edge of utilizing collective judgment of multiple techniques in one model. Post various iterations, TCPWave built ATLANTIS Model (The hybrid model with CNN, LSTM, and ANN techniques).

As the DGA generated domains, random alphanumeric character domains, are different from the legitimate traffic in structural, linguistic, and statistical properties, ML models are trained on derived feature queries. Meanwhile, the Deep Learning techniques have demonstrated the ability to find and extract these structural, linguistic, and statistical features. DL Models are trained on encoded query vectors. 3.5M records of malicious and non-malicious domains are used to train the models and these models perform well on their various training and testing sets and can generalize to new DGA families or new versions of previously seen families. The following diagram illustrates how TCPWave IPAM detects and prevents DGA in real-time:



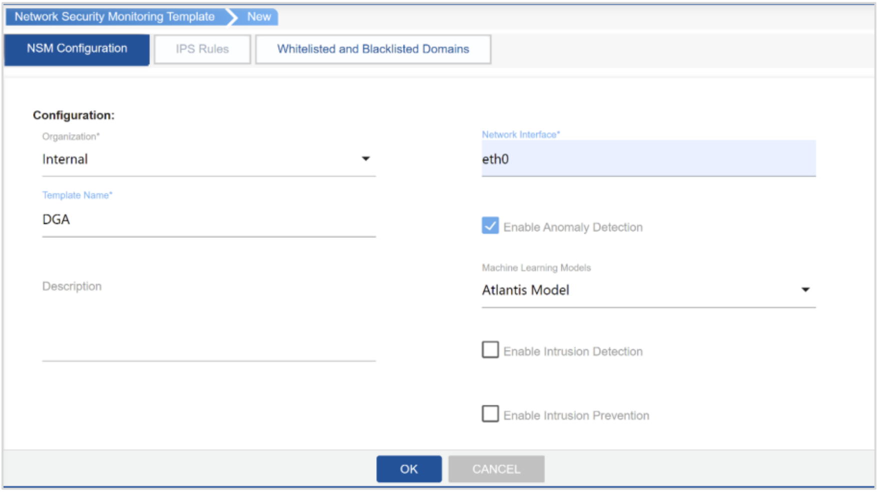
The following machine learning techniques are used in TCPWave IPAM:

- **Convolutional Neural Networks** (CNN) developed to analyze visual imagery data, works better with text data classification as well. It extracts higher representational features automatically from the data and trains models for better classification.
- **Long- and Short-Term Memory** (LSTM) networks are built for processing sequential data (such as speech and video). Extracts the features by processing the entire sequence of the query without treating each character independently and retaining long-term dependencies in the string.
- **Artificial Neural Networks** (ANN), computing systems analogous to biological neural networks in human brains, adds potential optimization to the huge list of feature vectors.
- **Decision Tree** (DT) classifies data by traversing through a tree structure, asking relevant questions about the data features; when the traversing reaches a leaf node, the data point is classified according to the class in the leaf node.
- **K-Nearest-Neighbors** (KNN) classifies new observations using the majority class of the K nearest observations in the training dataset.
- **Support Vector Machines** (SVM) uses hyperplanes in high dimensions to separate data into different classes.
- **Random Forest** (RF) aggregates and produces a mean of several Decision Trees trained from different random subsets of the training data.
- **Extremely Randomized Trees**(ET) It is also an Ensemble Algorithm. Works very much like Random Forest but randomness goes one step further in the way splits are computed.

DGA Detection Configuration in IPAM

The TCPWave IPAM allows the administrator to define the Network Security Monitoring templates to assign to individual TCPWave DNS Remote appliances. Network Security Monitoring templates allow the admin to select the desired Machine Learning model under “Enable Anomaly Detection”, to detect and prevent the DGA attack. The following Machine learning models are available:

- Atlantis (Recommended)
- Extremely Randomized Trees
- Random Forest
- SVM, Decision Tree & KNN
- Support Vector Machine


Network Security Monitoring Template
New
NSM Configuration
IPS Rules
Whitelisted and Blacklisted Domains
OK
CANCEL

Configuration:

Organization*: Internal

Template Name*: DGA

Description

Network Interface*: eth0

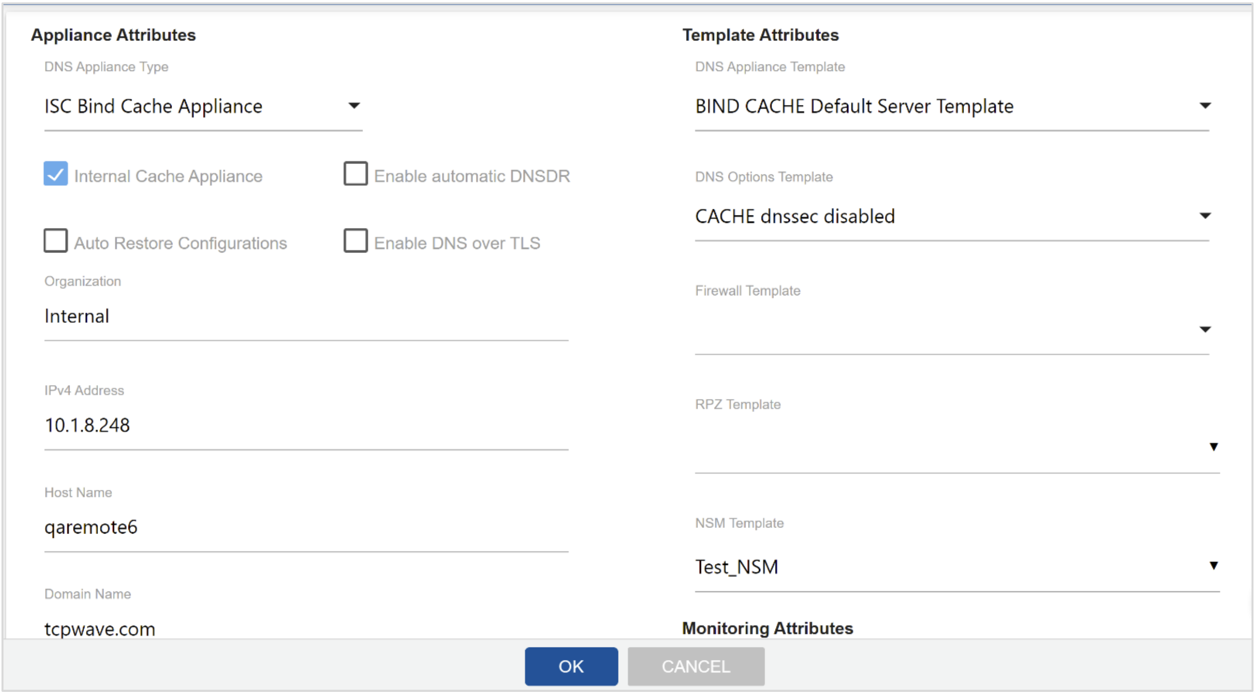
☑ Enable Anomaly Detection

Machine Learning Models: Atlantis Model

☐ Enable Intrusion Detection

☐ Enable Intrusion Prevention

Now associate the NSM template to the TCPWave DNS Remote appliances from the TCPWave DNS Appliances page.



Appliance Attributes

DNS Appliance Type: ISC Bind Cache Appliance

☑ Internal Cache Appliance ☐ Enable automatic DNSDR

☐ Auto Restore Configurations ☐ Enable DNS over TLS

Organization: Internal

IPv4 Address: 10.1.8.248

Host Name: qaremote6

Domain Name: tcpwave.com

Template Attributes

DNS Appliance Template: BIND CACHE Default Server Template

DNS Options Template: CACHE dnssec disabled

Firewall Template:

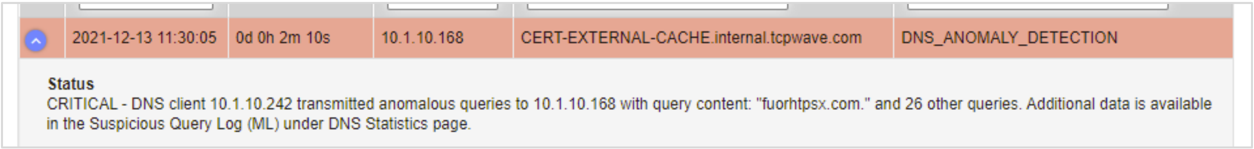
RPZ Template:

NSM Template: Test_NSM

Monitoring Attributes

Viewing Alerts and Logs

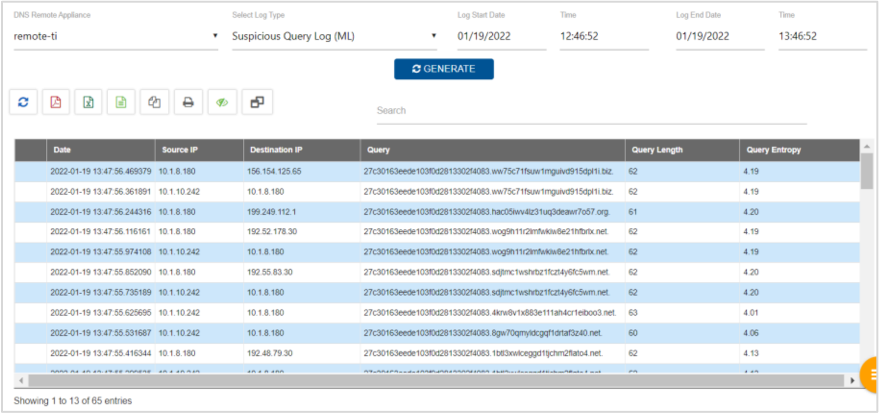
When an attack is detected, the system generates alerts in the TCPWave IPAM Dashboard. On setting the global parameters from the TCPWave IPAM Global Policy Management, the system prevents the DGA attacks in real-time.



2021-12-13 11:30:05	0d 0h 2m 10s	10.1.10.168	CERT-EXTERNAL-CACHE.internal.tcpwave.com	DNS_ANOMALY_DETECTION

Status
CRITICAL - DNS client 10.1.10.242 transmitted anomalous queries to 10.1.10.168 with query content: "fuorhtpsx.com." and 26 other queries. Additional data is available in the Suspicious Query Log (ML) under DNS Statistics page.

TCPWave DDI Admin has the privilege to view the DGA activity by fetching the Suspicious Query Log (ML) report of a remote DNS appliance.



DNS Remote Appliance: remote-ti

Select Log Type: Suspicious Query Log (ML)

Log Start Date: 01/19/2022 Time: 12:46:52

Log End Date: 01/19/2022 Time: 13:46:52

Date	Source IP	Destination IP	Query	Query Length	Query Entropy
2022-01-19 13:47:56.469379	10.1.8.180	156.154.125.65	27c30163eede103f0d2813302f4083.ww75c71fsuw1mguivd915dpl1i.biz.	62	4.19
2022-01-19 13:47:56.361891	10.1.10.242	10.1.8.180	27c30163eede103f0d2813302f4083.ww75c71fsuw1mguivd915dpl1i.biz.	62	4.19
2022-01-19 13:47:56.244316	10.1.8.180	199.249.112.1	27c30163eede103f0d2813302f4083.hac05iwv4lz31uq3deawr7o57.org.	61	4.20
2022-01-19 13:47:56.116161	10.1.8.180	192.52.178.30	27c30163eede103f0d2813302f4083.wog9h11r2lmfwkiw8e21hfbrlx.net.	62	4.19
2022-01-19 13:47:55.974108	10.1.10.242	10.1.8.180	27c30163eede103f0d2813302f4083.wog9h11r2lmfwkiw8e21hfbrlx.net.	62	4.19
2022-01-19 13:47:55.852090	10.1.8.180	192.55.83.30	27c30163eede103f0d2813302f4083.sdjtmc1wshrbz1fczt4y6fc5wm.net.	62	4.20
2022-01-19 13:47:55.735189	10.1.10.242	10.1.8.180	27c30163eede103f0d2813302f4083.sdjtmc1wshrbz1fczt4y6fc5wm.net.	62	4.20
2022-01-19 13:47:55.625695	10.1.10.242	10.1.8.180	27c30163eede103f0d2813302f4083.4krw8v1x883e111ah4cr1eiboo3.net.	63	4.01
2022-01-19 13:47:55.531687	10.1.10.242	10.1.8.180	27c30163eede103f0d2813302f4083.8gw70qmyldcgqf1drtaf3z40.net.	60	4.06
2022-01-19 13:47:55.416344	10.1.8.180	192.48.79.30	27c30163eede103f0d2813302f4083.1btl3xwlceggd1tjchm2flato4.net.	62	4.13

Showing 1 to 13 of 65 entries

Model Evaluation

The model evaluation section provides the metrics, model performance on various DGA families. TCPWave IPAM set of models predicts the accuracy of 88% - 98%. The following sub-sections describe one of the best model performances.

Model Performance

The model has performed great across the metrics on training and test datasets. Clocked Training accuracy of 0.9778, And on test accuracy is 0.9790, Precision, Recall and F1 Score 0.9867, 0.9799, 0.9833.

Performance on DGA families

We have validated the model performance on different DGA families and the following are the accuracy and False Negative ratio metrics.

DGA_class	Accuracy	FN_ratio
bamital	100	0
banjori	99.77	0.23
chinad	100	0
cryptolocker	99	1
dircrypt	98.96	1.04
dyre	100	0
emotet	99.68	0.32
enviserv	99.8	0.2
feodo	100	0
flubot	99.62	0.38
fobber_v1	100	0
fobber_v2	98.66	1.34
gameover	100	0
locky	96.72	3.28
murofet	99.79	0.21
mydoom	94.2	5.8
necro	98.71	1.29
necurs	97.84	2.16
padcrypt	97.02	2.98
pykspa_v1	97.48	2.52
pykspa_v2_fake	94	6
pykspa_v2_real	93.43	6.57
qadars	97.5	2.5
ramnit	98.33	1.67
ranbyus	99.58	0.42
rovnix	99.97	0.03
shifu	91.08	8.92
shiotob	98.93	1.07
simda	97.84	2.16

DGA_class	Accuracy	FN_ratio
symmi	99.51	0.49
tempedreve	91.19	8.81
tinba	99.63	0.37
tordwm	91.18	8.82

Note: Ignored the metrics of the DGA families, for the domains less than 100.

Conclusion

Armed with this information, network administrators can plan and govern their DNS environment, accelerating IP space provisioning and management, simplifying configuration, supporting zero-touch automation initiatives, and strengthening corporate cybersecurity posture.

Appendix

The machine learning modules are evaluated using the following metrics:
Accuracy = (TP+TN)/(TP+TN+FP+FN)
Precision = TP/(TP+FP)
Recall = TP/(TP+FN)
F1 Score = (2*Precision*Recall)/ (Precision+ Recall)
False Negative Ratio (also called as Miss Rate) = FN/(FN+TP)

- True positive = TP
- True negative = TN
- False positive = FP
- False negative (FN)