UNIVERSITÀ DEGLI STUDI DI MILANO - BICOCCA
Scuola di Scienze
Dipartimento di Informatica, Sistemistica e Comunicazione
Corso di Laurea in Informatica

Adozione di Tecniche di Machine Learning per l'Identificazione di Intrusioni nelle Reti di Telecomunicazioni

Relatore: Dott. Marco Savi

Correlatore: Jacopo Talpini

Laureando:

Nicolò Urbani

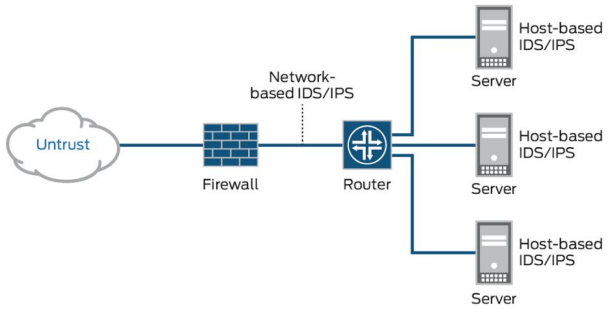
856213

Analisi Problema e Obiettivi

- Problema :

  Aumento Attacchi Informatici nelle Reti

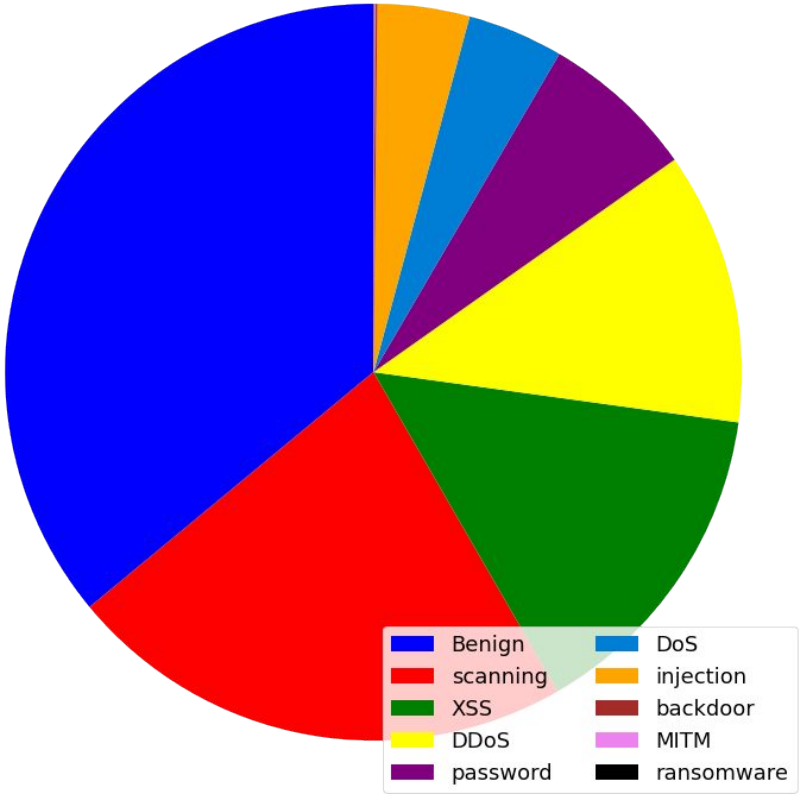
  di Telecomunicazione



- **Network Intrusion Detection System** (NIDS) cosa sono ?
  - Monitorare i flussi di rete
  - Individuare pattern per il riconoscimento automatico degli attacchi
- Obiettivi:
  - Analizzare e Confrontare diverse tecniche di **Supervised Machine Learning** su diversi Dataset IDS

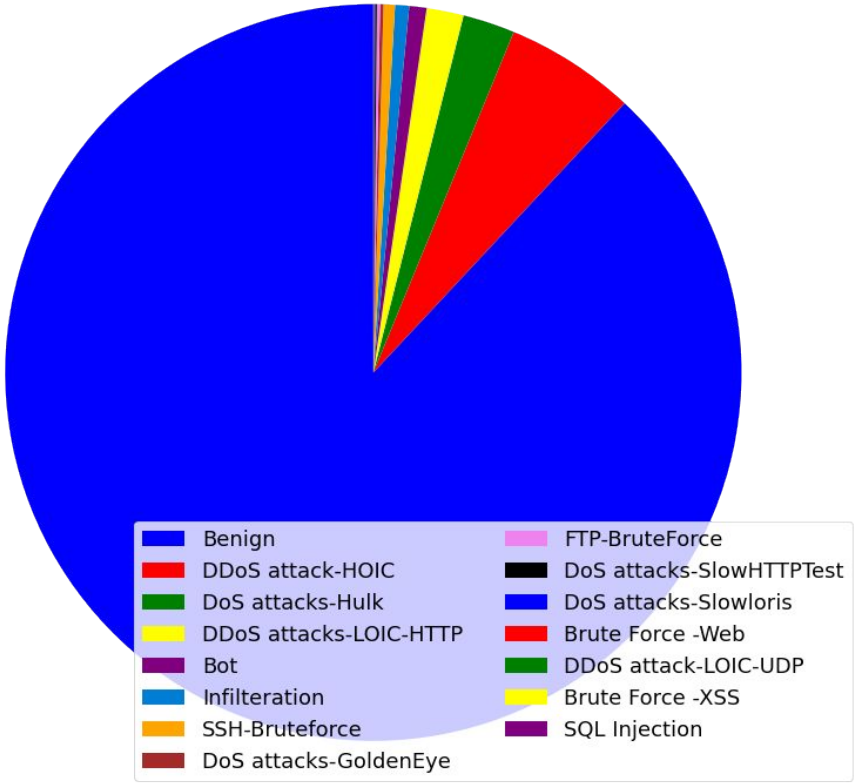
    ➜ **Modello più Performante**
  - Valutare il comportamento del modello combinando più dataset

NF-TON-IoT-v2



36% Traffico Benigno

NF-CSE-CIC-IDS2018-v2



88% Traffico Benigno

Sample Dataset NF-TON-IoT-v2

- 43 Features -Standard NetFlow-Versione 2 (CISCO)
- 8.5 milioni di dati

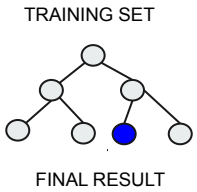
- Estratto del dataset NF-TON-IoT-v2 :

43 Features

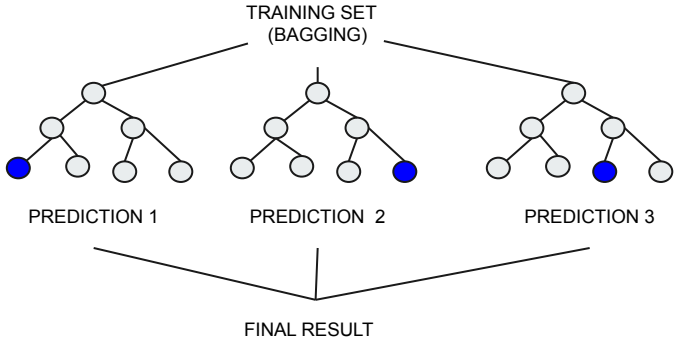
8.5 milioni

IPV4_SRC_ADDR	L4_SRC_PORT	IPV4_DST_ADDR	L4_DST_PORT	L7_PROTO	IN_BYTES	IN_PKTS	OUT_BYTES	LONGEST_FLOW_PKT	...	Label
192.168.1.169	65317	239.255.255.250	1900	0	165	1	0	165		Benign
192.168.1.79	54023	192.168.1.255	53	0	108	2	108	54		DoS
192.168.1.169	41754	239.255.255.250	3766	0	48	1	0	48		Scanning

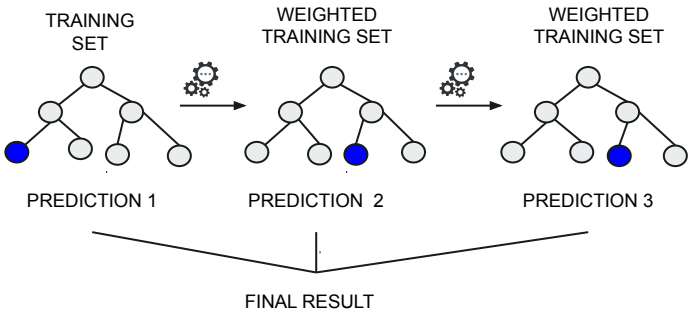
Tecniche di Machine Learning



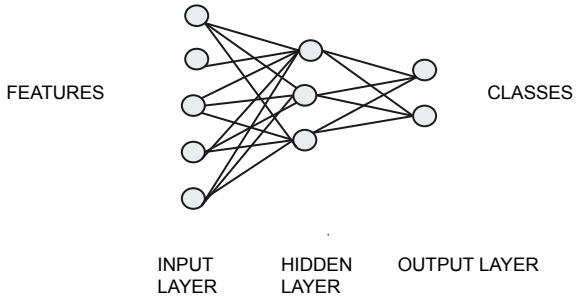
Decision Tree



Random Forest / Extra Trees



Boosted Decision Tree



Neural Network

Confronto Modelli: NF-TON-IoT-v2 - Test Set

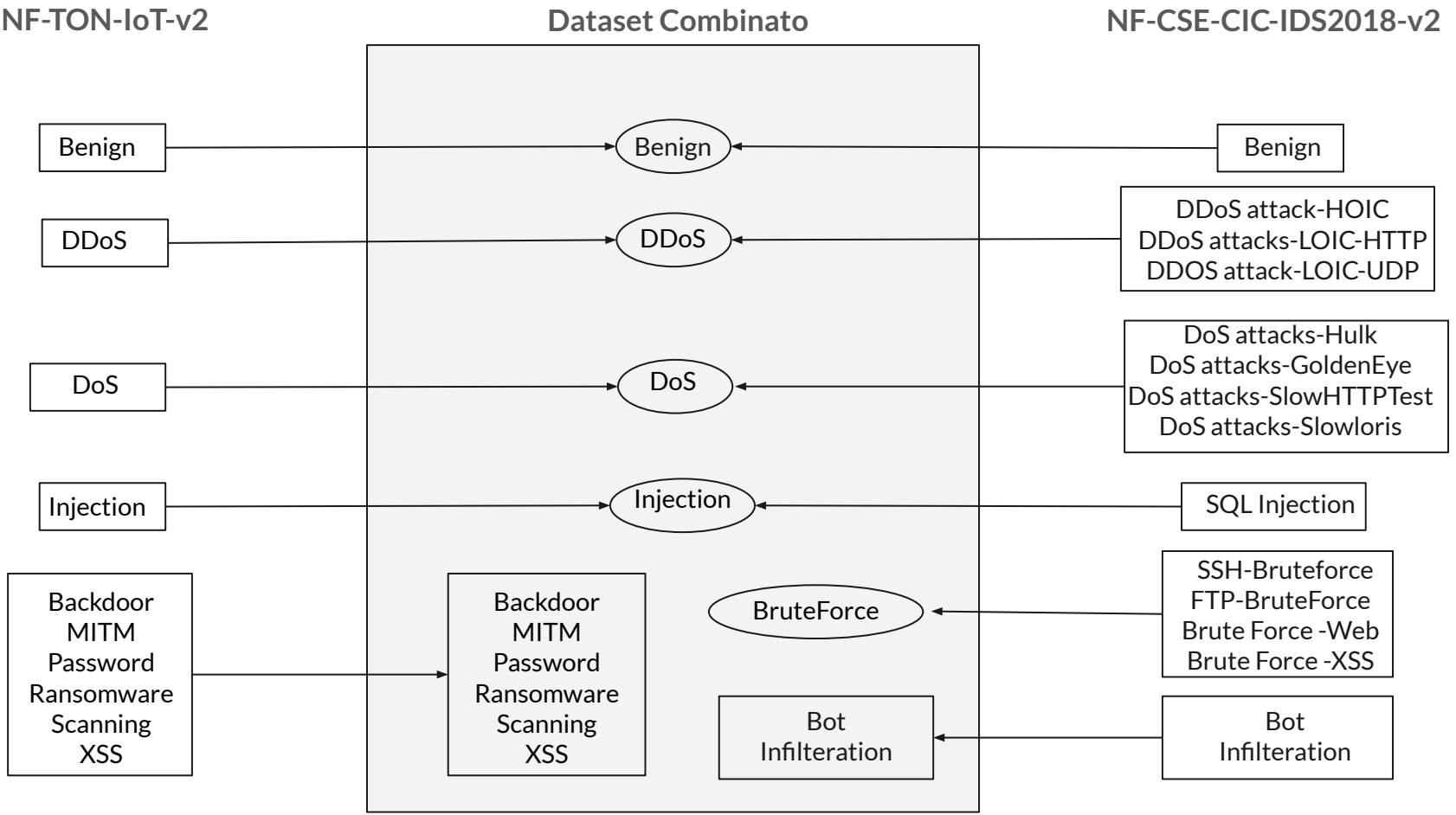
Performance Metrics		Decision Tree	Random Forest	Extra Trees	Boosted DT	Neural Network
Precision	Macro AVG	0.9212	0.9698	0.9498	0.9224	0.7388
	Weighted AVG	0.9752	0.9822	0.9812	0.9752	0.9448
Recall	Macro AVG	0.9171	0.9024	0.9013	0.9173	0.8722
	Weighted AVG	0.9751	0.9820	0.9811	0.9752	0.9259
F1	Macro AVG	0.9191	0.9216	0.9175	0.9197	0.7485
	Weighted AVG	0.9752	0.9819	0.9810	0.9752	0.9346
Accuracy		0.9751	0.9820	0.9811	0.9751	0.9259
Percentage False Benign		0.68%	0.30%	0.32%	0.67%	1.72%
Model Fitting Time (s)		89.13	234.9	305.3	89.74	145.44
Prediction Time(µs)		0.21	6.66	6.03	0.47	1.38

Random Forest NF-TON-IoT-v2

	precision	recall	f1-score	support
Benign	0.9970	0.9938	0.9954	609947
backdoor	0.9994	0.9952	0.9973	1681
DDoS	0.9925	0.9872	0.9898	202624
DoS	0.9269	0.9081	0.9174	71261
injection	0.9576	0.8918	0.9235	68446
MITM (Man In The Middle)	0.9420	0.3368	0.4962	772
password	0.9746	0.9680	0.9713	115333
ransomware	0.9706	0.9649	0.9677	342
scanning	0.9971	0.9960	0.9966	378142
XSS (Cross Site Scripting)	0.9404	0.9821	0.9608	245502
Accuracy			0.9820	1694050
Macro AVG	0.9698	0.9024	0.9216	1694050
Weighted AVG	0.9822	0.9820	0.9819	1694050

ARP Poisoning
Port stealing
ICMP Redirection

Combinazione Dataset



Scenari - Combinazione Dataset

Scenario 1

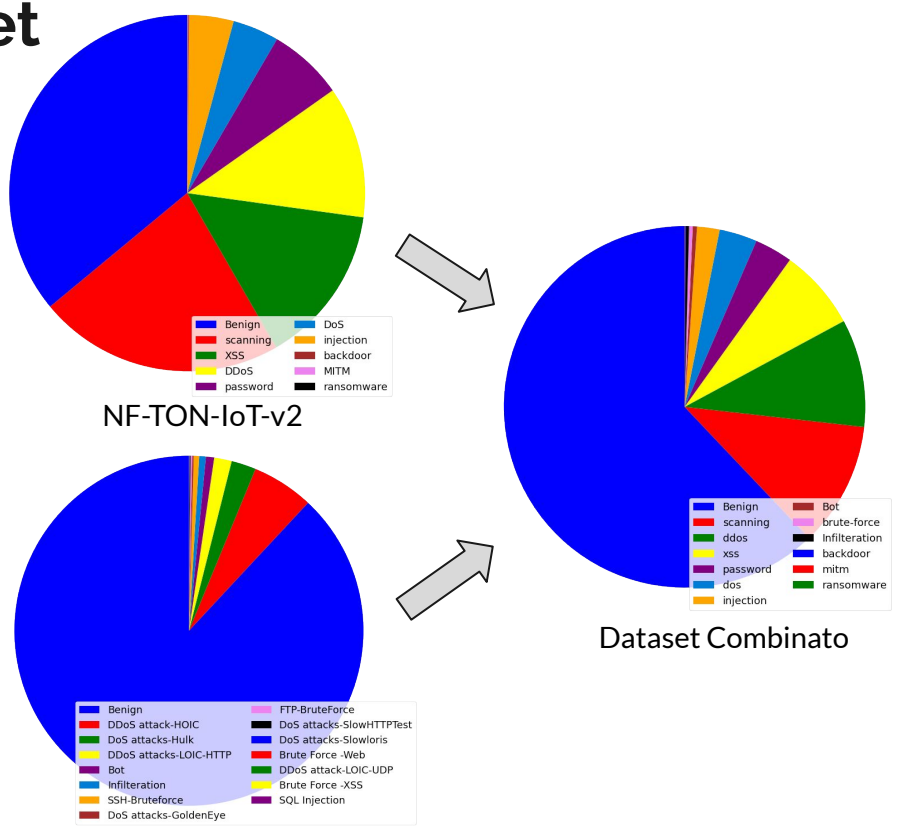
- **Training Set :** Dataset Combinato
- **Test Set**: Dataset Combinato

Scenario 2

- **Training Set :** Dataset Combinato
- **Test Set**: NF-CSE-CIC-IDS2018-v2

Scenario 3

- **Training Set :** NF-TON-IoT-v2
- **Test Set**: NF-CSE-CIC-IDS2018-v2



Confronto Scenari: Test Set

Performance Metrics		Scenario 1	Scenario 2	Scenario 3
Precision	Macro AVG	0.9718	0.9370	0.2362
	Weighted AVG	0.9878	0.9973	0.8491
Recall	Macro AVG	0.8683	0.8637	0.2319
	Weighted AVG	0.9878	0.9971	0.8336
F1	Macro AVG	0.8960	0.8925	0.2334
	Weighted AVG	0.9872	0.9969	0.8413

Accuracy	0.9877	0.9971	0.8345
Percentage False Benign	0.46%	2.69%	5.52%
Model Fitting Time (s)	289.96	469.00	376.87
Prediction Time (µs)	6.17	10.47	5.86

Osservazioni Conclusive

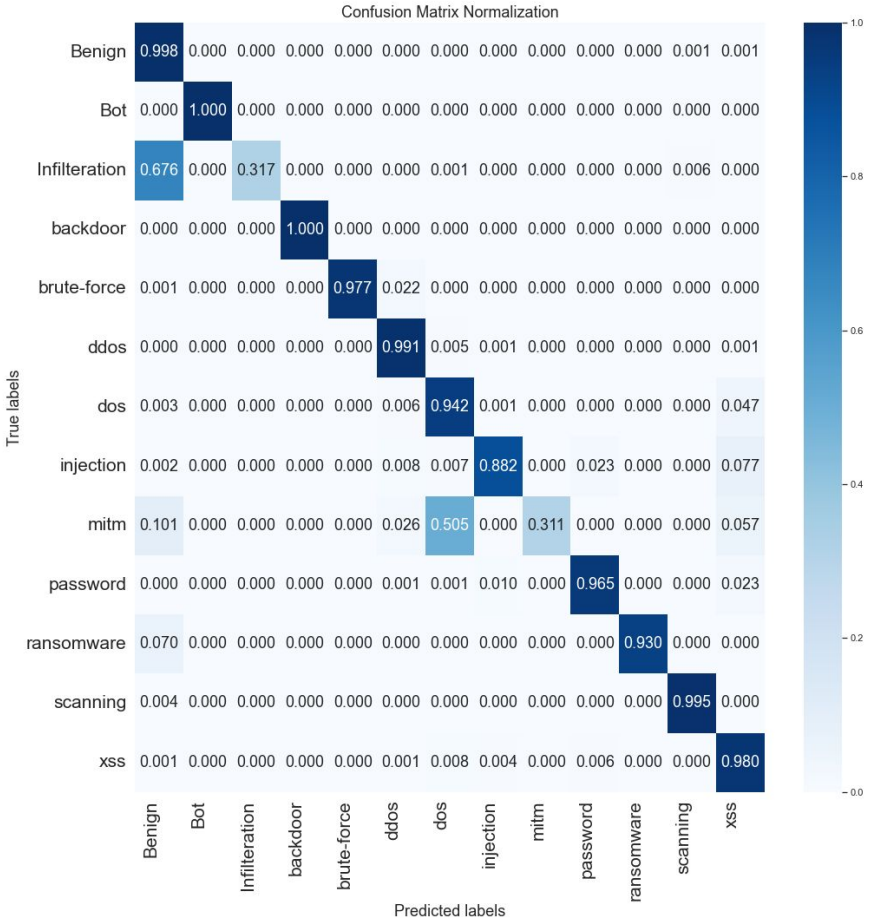
- Applicare e Confrontare Tecniche di Machine Learning su Dataset presenti in letteratura
- Modello più performante: **Random Forest** ➜ Performance confrontabili con i lavori dello stato dell'arte
- Aspetti Cruciali:
  - Schemi di Attacco
  - Etichettatura del Dataset
  - Sbilanciamento del Dataset
- **Ulteriori Sviluppi futuri**: Federated Learning (FL)
  - Addestramento Locale
  - Efficienza Computazionale e Privacy

GRAZIE PER L’ ATTENZIONE

Approfondimenti

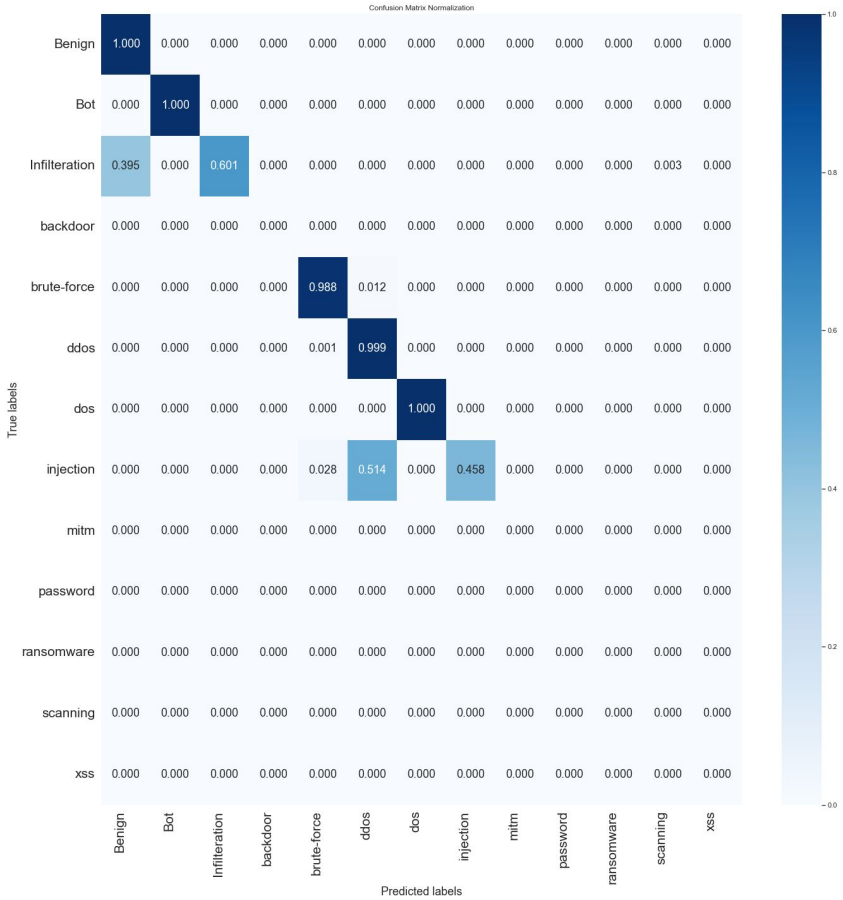
Scenario 1

	precision	recall	f1-score	support
Benign	0.9954	0.9976	0.9965	1053574
Bot	1.0000	1.0000	1.0000	6440
Infilteration	0.9584	0.3168	0.4762	5236
backdoor	0.9988	1.0000	0.9994	840
brute-force	0.9920	0.9774	0.9847	5579
ddos	0.9942	0.9914	0.9928	163874
dos	0.9513	0.9419	0.9466	57411
injection	0.9541	0.8819	0.9166	34243
mitm	0.9160	0.3109	0.4642	386
password	0.9713	0.9645	0.9679	57666
ransomware	0.9695	0.9298	0.9493	171
scanning	0.9957	0.9952	0.9954	189071
xss	0.9368	0.9799	0.9578	122751
Accuracy			0.9878	1697242
Macro AVG	0.9718	0.8683	0.8960	1697242
Weighted AVG	0.9878	0.9878	0.9872	1697242



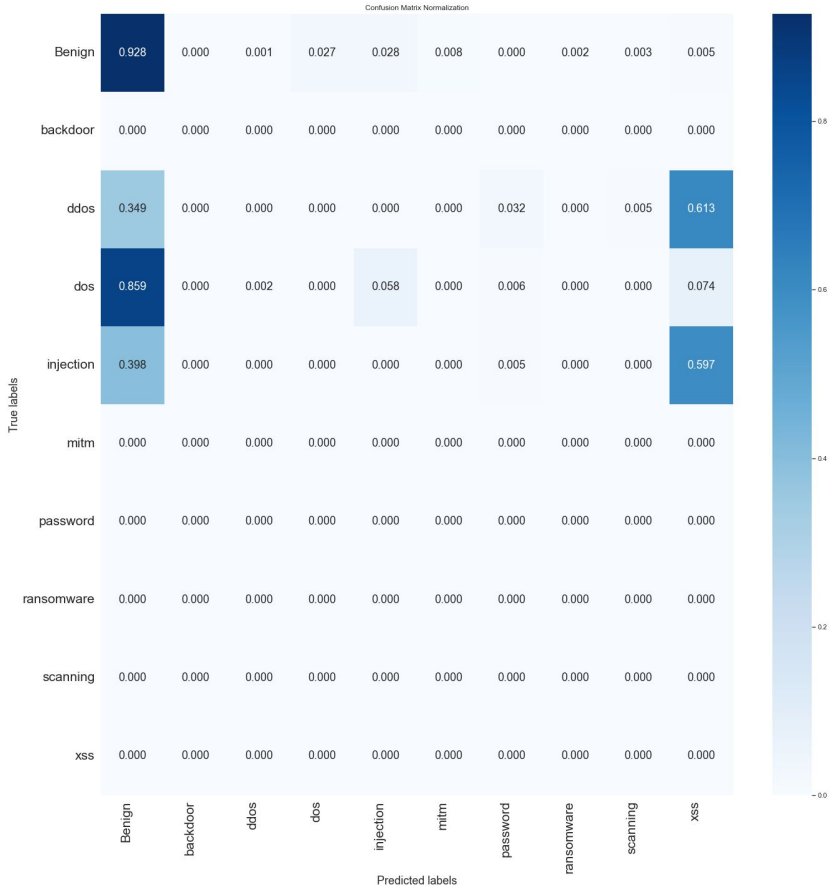
Scenario 2

	precision	recall	f1-score	support
Benign	0.9972	0.9996	0.9984	8317784
Bot	1.0000	1.0000	1.0000	71548
Infilteration	0.9879	0.6014	0.7476	58180
brute-force	0.9929	0.9876	0.9903	61992
ddos	0.9987	0.9993	0.9990	695135
dos	0.9966	1.0000	0.9983	242000
injection	0.5858	0.4583	0.5143	216
Accuracy			0.9971	9446855
Macro AVG	0.9370	0.8637	0.8925	9446855
Weighted AVG	0.9973	0.9971	0.9969	9446855



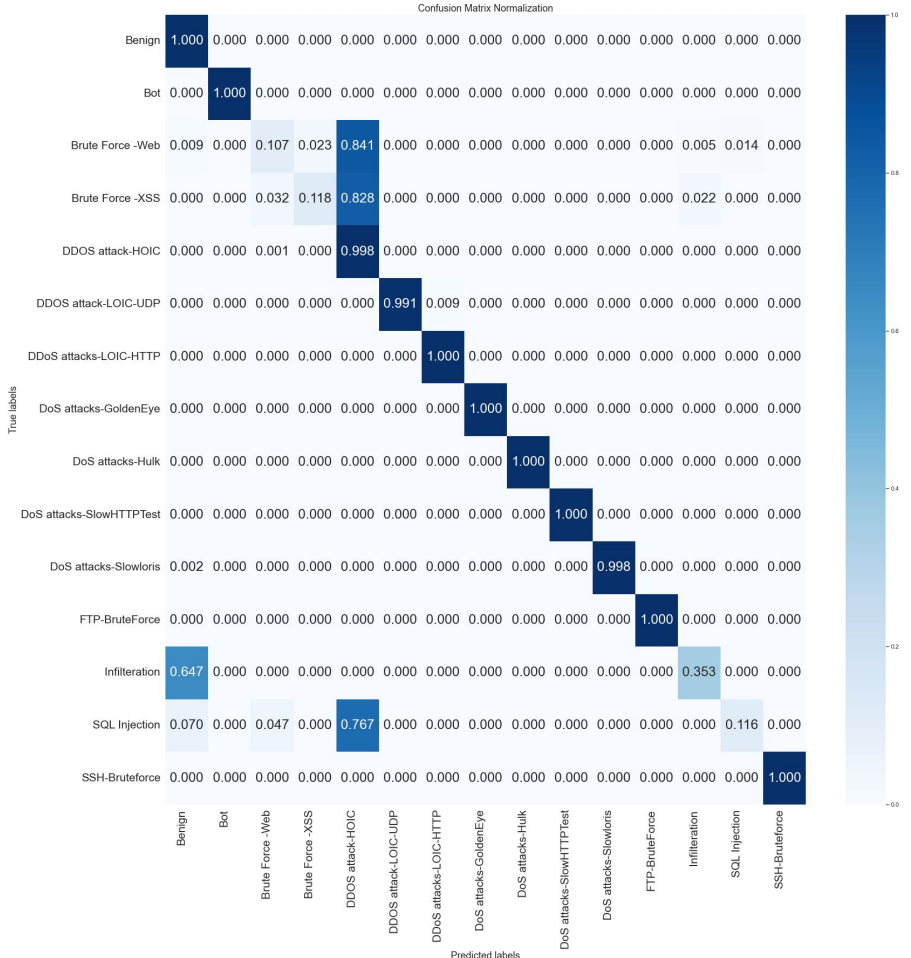
Scenario 3

	precision	recall	f1-score	support
Benign	0.9448	0.9275	0.9336	8317784
ddos	0.0000	0.0000	0.0000	695135
dos	0.0001	0,0001	0.0001	242000
injection	0.0000	0.0000	0.0000	216
Accuracy			0.8336	9255135
Macro AVG	0.2362	0.2319	0.2334	9255135
Weighted AVG	0.8491	0.8336	0.8390	9255135

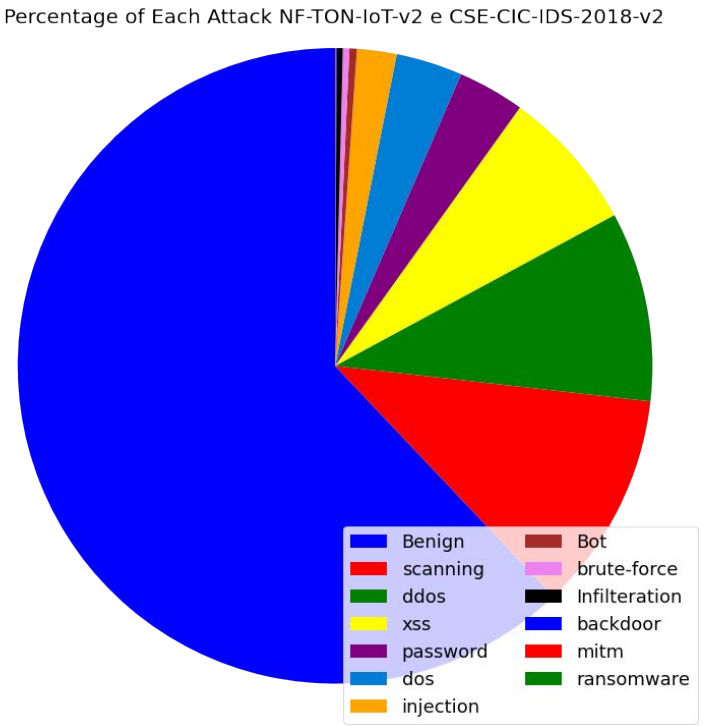


CSE-CID-IDS2018 Random Forest

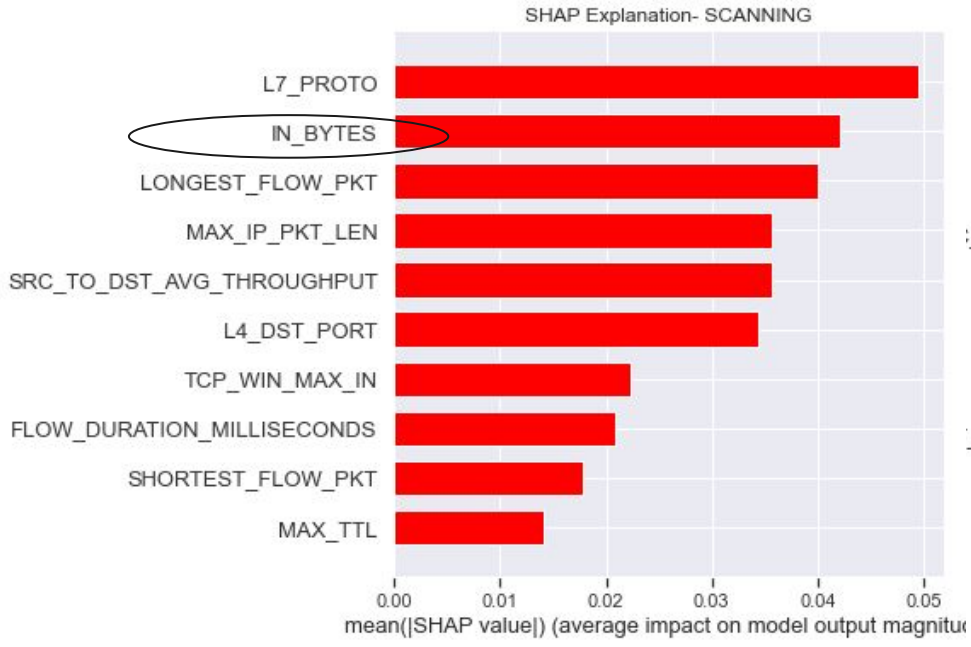
	precision	recall	f1-score	support
Benign	1.00	1.00	1.00	1663557
Bot	1.00	1.00	1.00	14310
Brute Force -Web	0.16	0.11	0.13	214
Brute Force -XSS	0.19	0.12	0.15	93
DDOS attack-HOIC	1.00	1.00	1.00	108086
DDOS attack-LOIC-UDP	1.00	0.99	0.99	211
DDoS attacks-LOIC-HTTP	1.00	1.00	1.00	30730
DoS attacks-GoldenEye	1.00	1.00	1.00	2772
DoS attacks-Hulk	1.00	1.00	1.00	43265
DoS attacks-SlowHTTPTest	1.00	1.00	1.00	1412
DoS attacks-Slowloris	1.00	1.00	1.00	951
FTP-BruteForce	1.00	1.00	1.00	2593
Infilteration	0.97	0.35	0.52	11636
SQL Injection	0.21	0.12	0.15	43
SSH-Bruteforce	1.00	1.00	1.00	9498
accuracy			1.00	1889371
macro avg	0.83	0.78	0.80	1889371
weighted avg	1.00	1.00	0.99	1889371

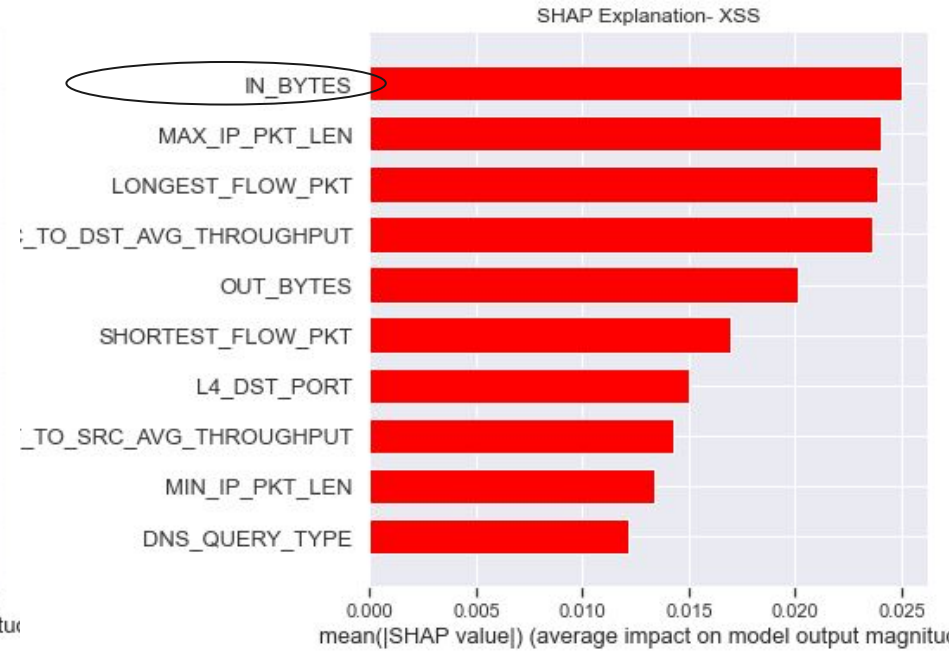


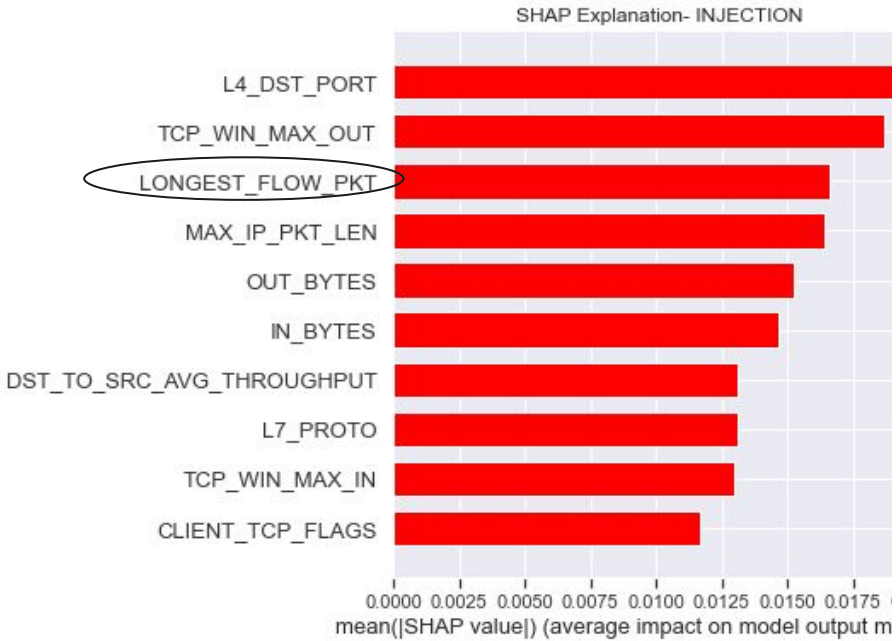
Combinazione Dataset CSE-CID-IDS2018 e NF-TON-IoT-v2

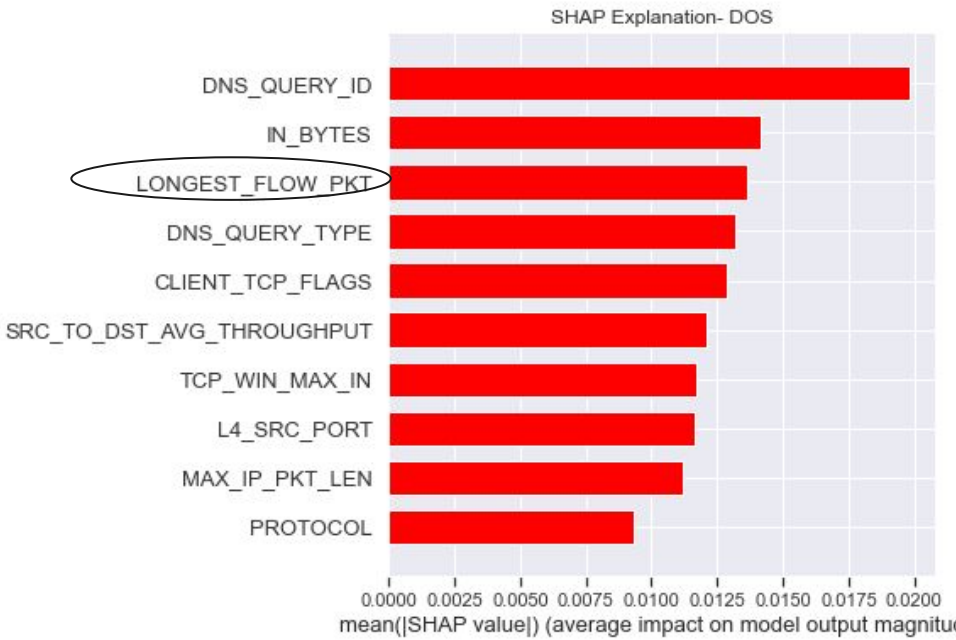


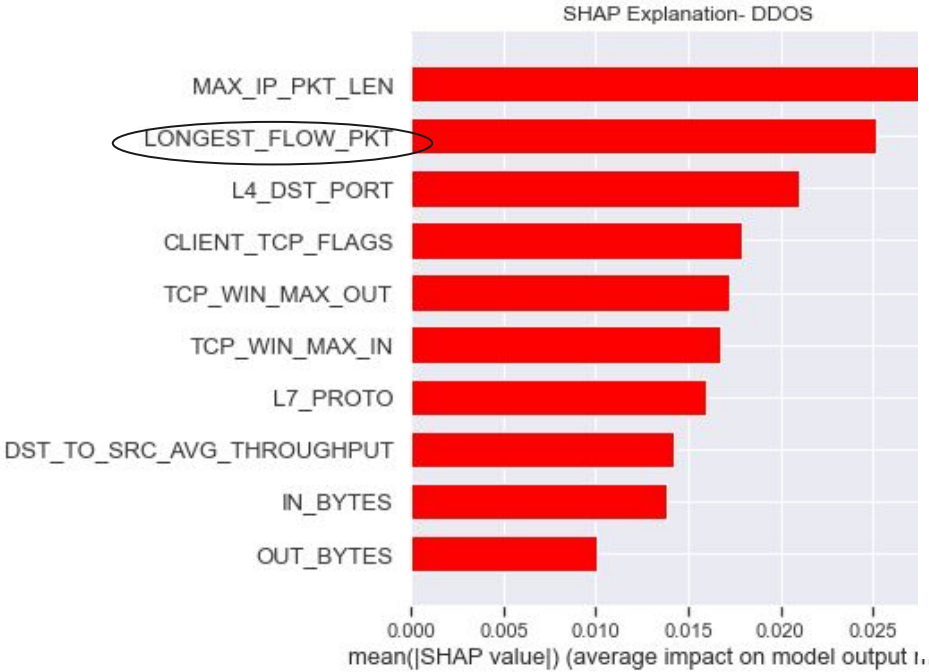
SHAP EXPLANATION NF-TON-IoT-v2

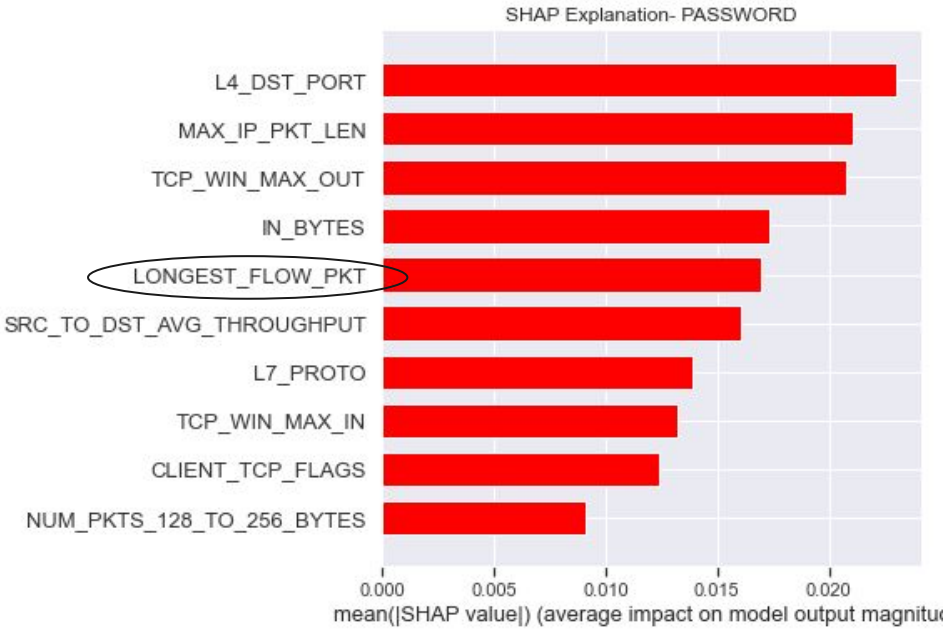





SHAP Explanation- INJECTION
L4_DST_PORT
TCP_WIN_MAX_OUT
LONGEST_FLOW_PKT
MAX_IP_PKT_LEN
OUT_BYTES
IN_BYTES
DST_TO_SRC_AVG_THROUGHPUT
L7_PROTO
TCP_WIN_MAX_IN
CLIENT_TCP_FLAGS
0.0000 0.0025 0.0050 0.0075 0.0100 0.0125 0.0150 0.0175
mean(|SHAP value|) (average impact on model output m


SHAP Explanation- DOS
DNS_QUERY_ID
IN_BYTES
LONGEST_FLOW_PKT
DNS_QUERY_TYPE
CLIENT_TCP_FLAGS
SRC_TO_DST_AVG_THROUGHPUT
TCP_WIN_MAX_IN
L4_SRC_PORT
MAX_IP_PKT_LEN
PROTOCOL
0.0000 0.0025 0.0050 0.0075 0.0100 0.0125 0.0150 0.0175 0.0200
mean(|SHAP value|) (average impact on model output magnitu


SHAP Explanation- DDOS
MAX_IP_PKT_LEN
LONGEST_FLOW_PKT
L4_DST_PORT
CLIENT_TCP_FLAGS
TCP_WIN_MAX_OUT
TCP_WIN_MAX_IN
L7_PROTO
DST_TO_SRC_AVG_THROUGHPUT
IN_BYTES
OUT_BYTES
0.000
0.005
0.010
0.015
0.020
0.025
mean(|SHAP value|) (average impact on model output


SHAP Explanation- PASSWORD
L4_DST_PORT
MAX_IP_PKT_LEN
TCP_WIN_MAX_OUT
IN_BYTES
LONGEST_FLOW_PKT
SRC_TO_DST_AVG_THROUGHPUT
L7_PROTO
TCP_WIN_MAX_IN
CLIENT_TCP_FLAGS
NUM_PKTS_128_TO_256_BYTES
0.000
0.005
0.010
0.015
0.020
mean(|SHAP value|) (average impact on model output magnitu