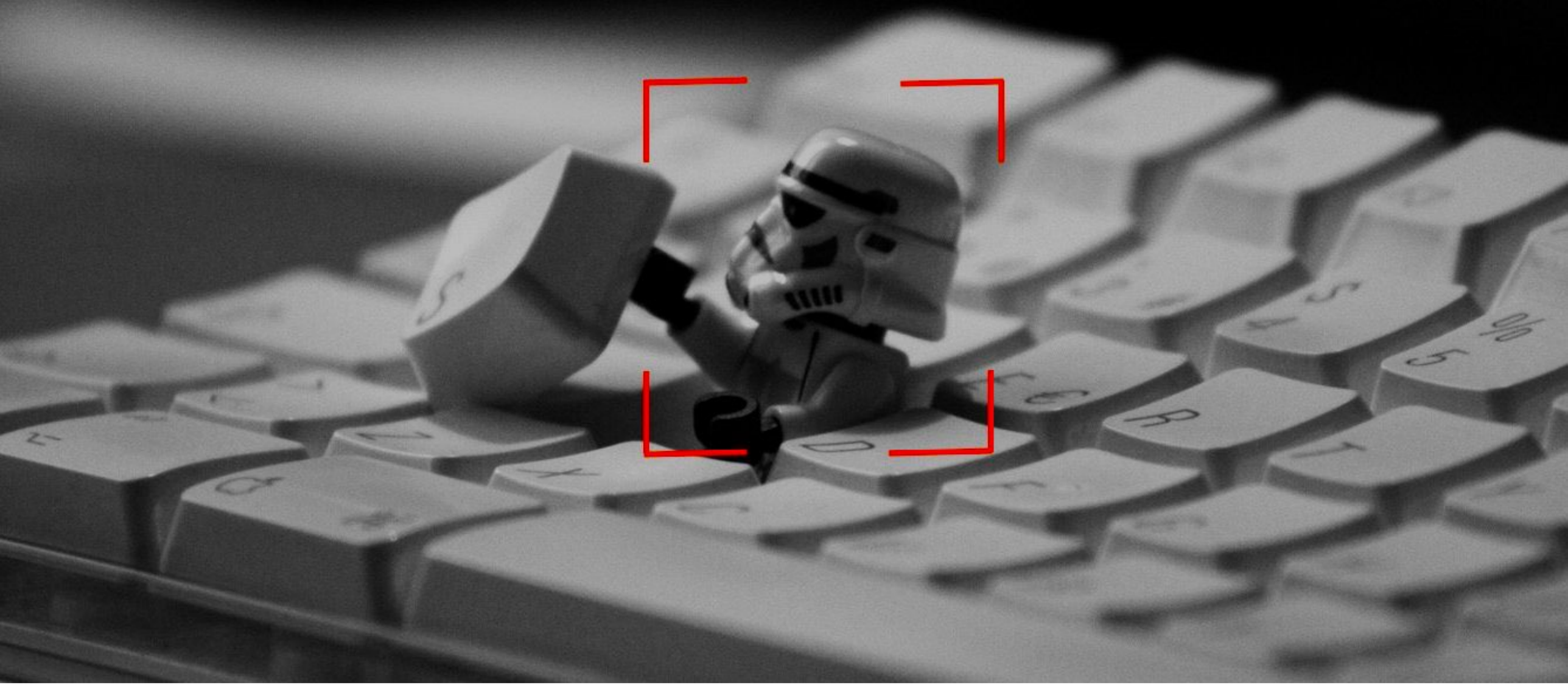


ZED-IDS

Un sistema di rilevamento delle intrusioni basato sul deep learning

Marta Catillo

09 ottobre 2019, workshop GARR

Consortium GARR

UNIVERSITÀ DEGLI STUDI DEL SANNIO
Benevento
DING
DIPARTIMENTO DI INGEGNERIA

Adult population of 20 countries - 3.1 billion

Online population (57%) - 1.8 billion

Experienced Cybercrime - 978 million

Source: Norton Cyber Security Insights Report 2018

Panorama Attuale (1)

Wikipedia @Wikipedia · 7 set

Wikipedia has been experiencing intermittent outages today as a result of a malicious attack. We're continuing to work on restoring access.
#wikipediadown

83 389 947

la Repubblica R+

Attacco hacker alla drone race: i quadricotteri fuori costretti ad atterraggi di emergenza

Cresce cybercrime, bersagliata la Sanità

Rapporto Clusit, "siamo a due minuti dalla mezzanotte"

Redazione ANSA

ROMA

03 ottobre 2019
11:06

NEWS

Suggerisci

Facebook

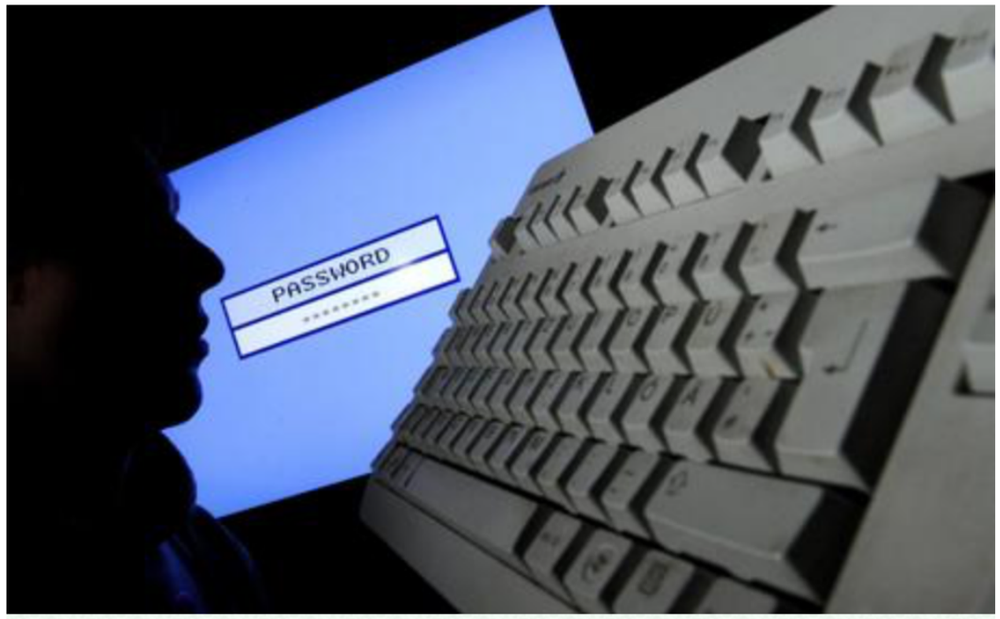
Twitter

Altri

A+ A A-

Stampa

Scrivi alla redazione



© ANSA/EPA

CLICCA PER INGRANDIRE

Panorama Attuale (2)

- esponenziale aumento dei network data
- incremento dei dispositivi connessi
  - popolarità dell’IoT
  - utilizzo esteso dei servizi cloud-based
- entro il 2020 la quantità di dati esistenti supererà i 44 ZB

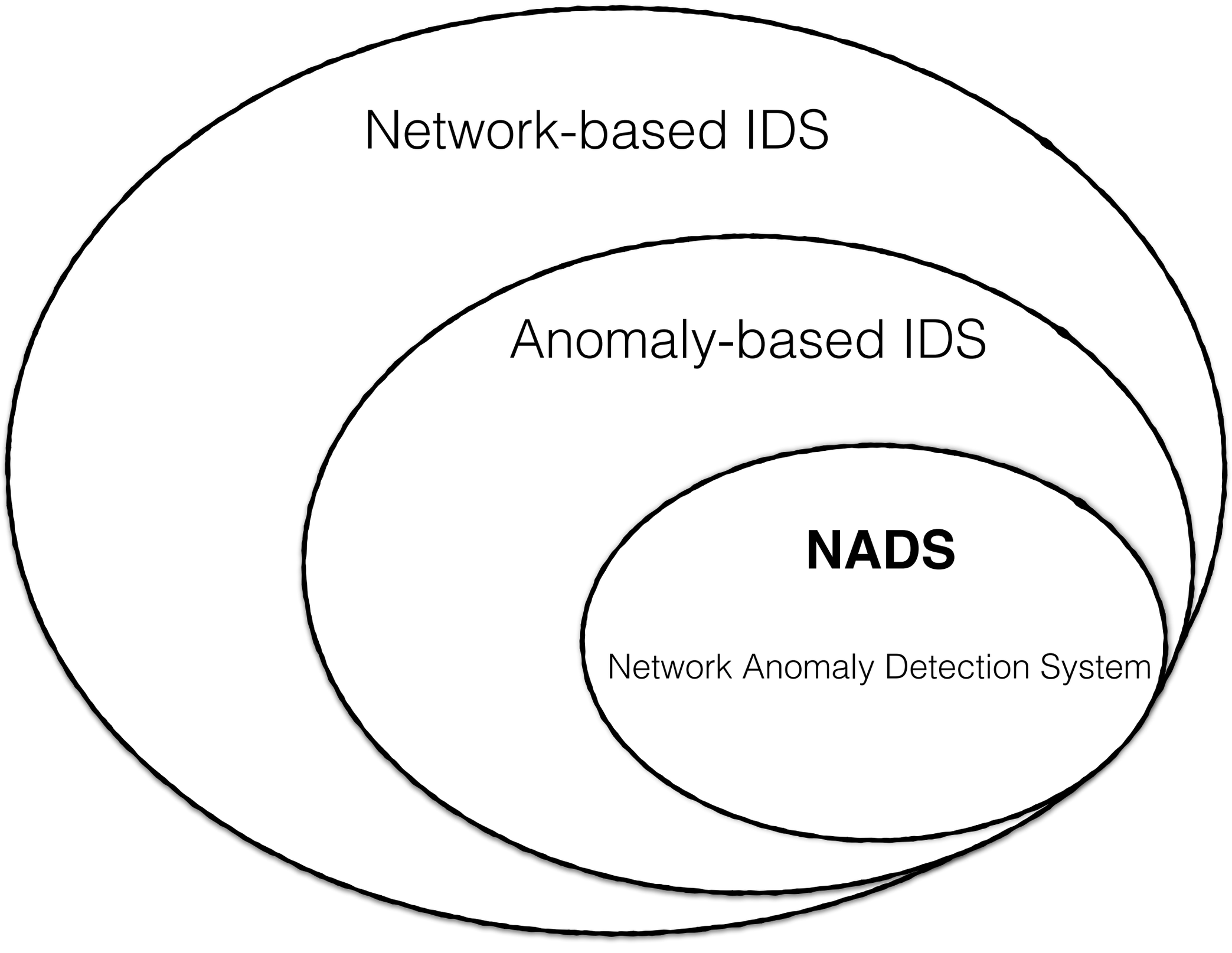
Challenge

Riconoscere gli attacchi di rete

IDS

Intrusion Detection System

ZED-IDS


Network-based IDS
Anomaly-based IDS
NADS
Network Anomaly Detection System

Dataset

Dataset (1)
CICIDS2017

- Dataset di dominio pubblico pensato per gli IDS
- Riproduce traffico reale
- Contiene sia traffico benigno che attacchi noti ed aggiornati

CSE-CIC-IDS2018

nasce da una collaborazione tra Communications Security Establishment (CSE) & the Canadian Institute for Cybersecurity (CIC)

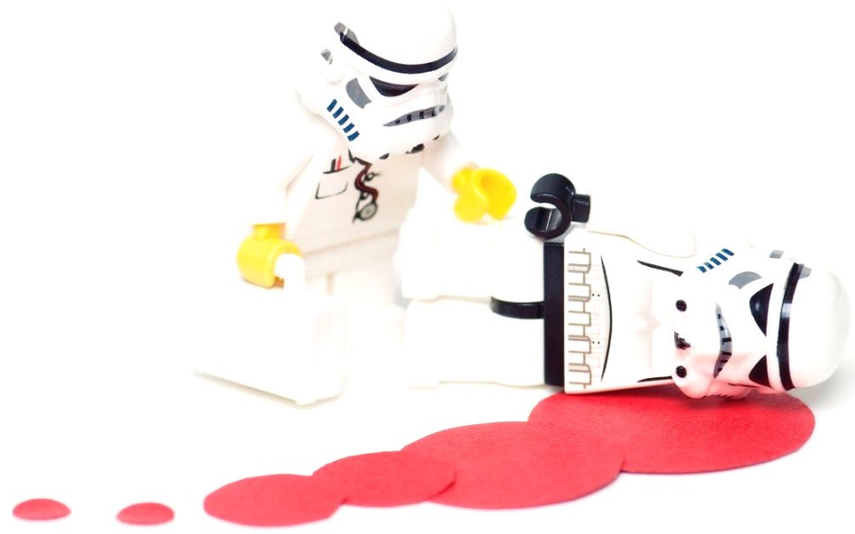
https://www.unb.ca/cic/datasets/ids-2017.html

CICIDS2017	CSE-CIC-IDS2018
Rete vittima: 3 server, 1 firewall, 2 switch, 10 PC	***Rete vittima:*** organizzata in 5 dipartimenti con 420 macchine e 30 server (piattaforma AWS)
Rete di attacco: 1 router, 1 switch, 4 PC	***Rete di attacco:*** 50 macchine

Dataset (2)
Attacchi

Periodo di cattura

- **start:** lunedì 3 luglio 2017 (9 a.m.)
- **end:** venerdì 7 luglio 2017 (5 p.m.)

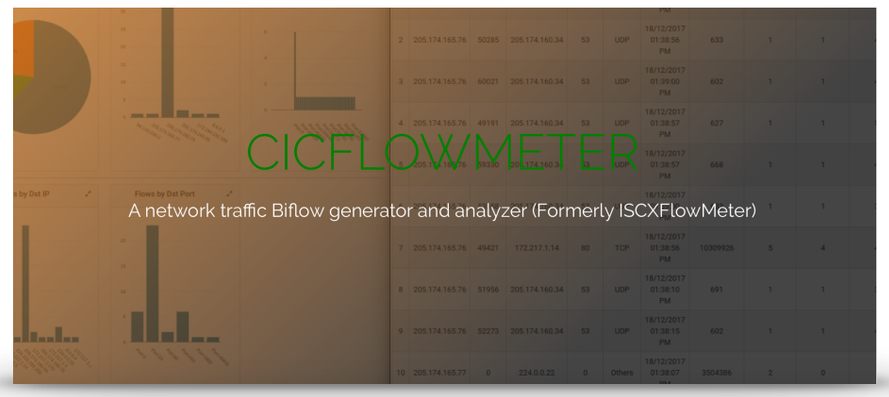


Giorno	Descrizione	Tipologia attacco
Lunedì	Normal activity	
Martedì	Attacks + Normal Activity	BForce, SFTP, SSH
Mercoledì	Attacks + Normal Activity	DoS, Heartbleed
Giovedì	Attacks + Normal Activity	Web and Infiltration attacks
Venerdì	Attacks + Normal Activity	Botnet, DDoS, PortScans

Dataset (3)
Formato

Flusso generato con **CICFLOWMETER**

- flusso bidirezionale
- identificato da 85 feature
- terminazione:
    - chiusura della connessione TCP
    - flow timeout per UDP

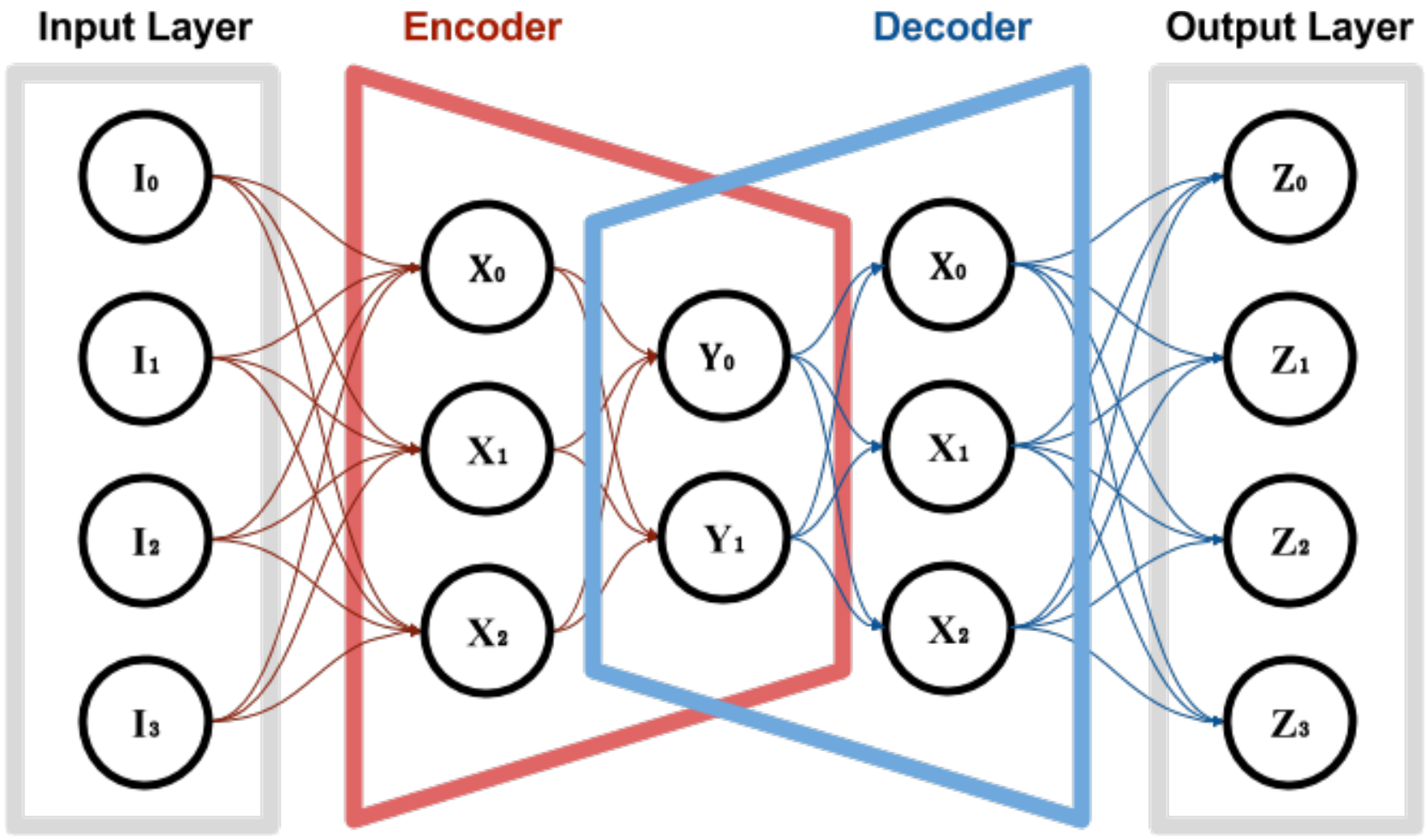


- File **pcap** per ogni singola giornata
- File **csv** contenenti flussi labelizzati

CICFLOWMETER
Input: file pcap per ogni singola giornata
Output: file csv contentente flussi (singolo record) e **feature** estratte

Metodologia

Autoencoder (1)



Encoder: tenta di rappresentare l'input dato con un numero minore di unità.
Decoder: tenta di rigenerare l'input utilizzando le informazioni codificate nei suoi livelli nascosti.

Autoencoder (2)

- Il livello di input ha la stessa dimensione del livello di output.
- Il livello nascosto impara la rappresentazione latente del vettore di input in uno spazio di feature differente con dimensioni più piccole.

- training task: cogliere le feature rilevanti dai dati di training nel bottleneck layer, in modo che l'input possa essere ricostruito nel livello di output.

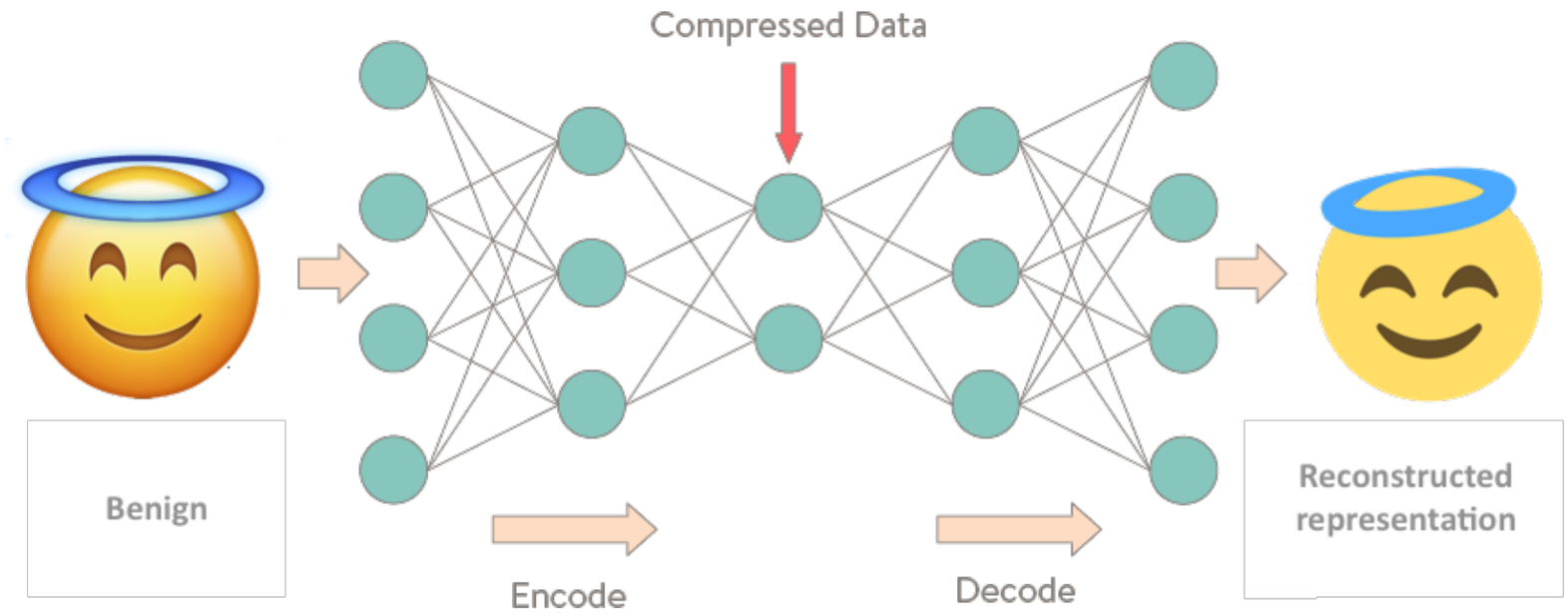
- Gli autoencoder sono addestrati con l'obiettivo di ridurre il loro RE.

- L'errore di ricostruzione (RE) è la differenza tra l'input ricostruito e la sua versione originale.

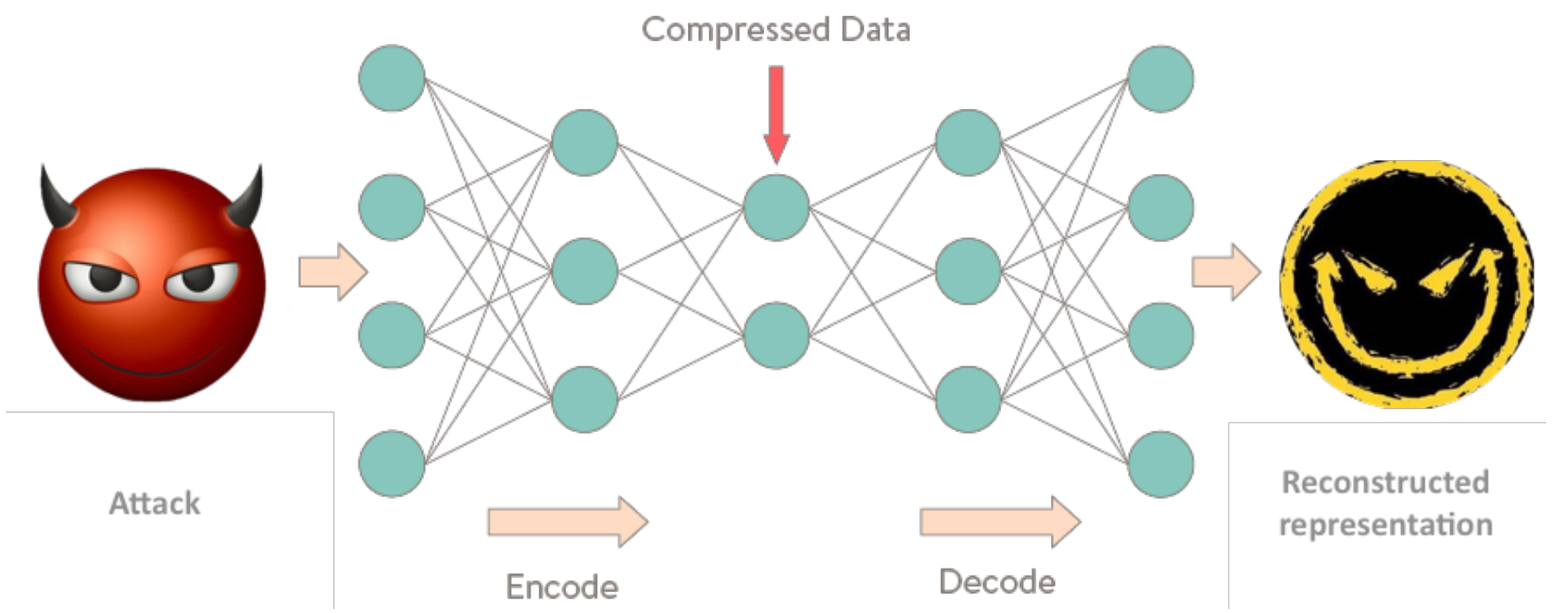
$$SSE = \sum_{i=1}^{n} (z_i - x_i)^2$$

Metodologia

Training set: solo record BENIGN



Low Reconstruction Error

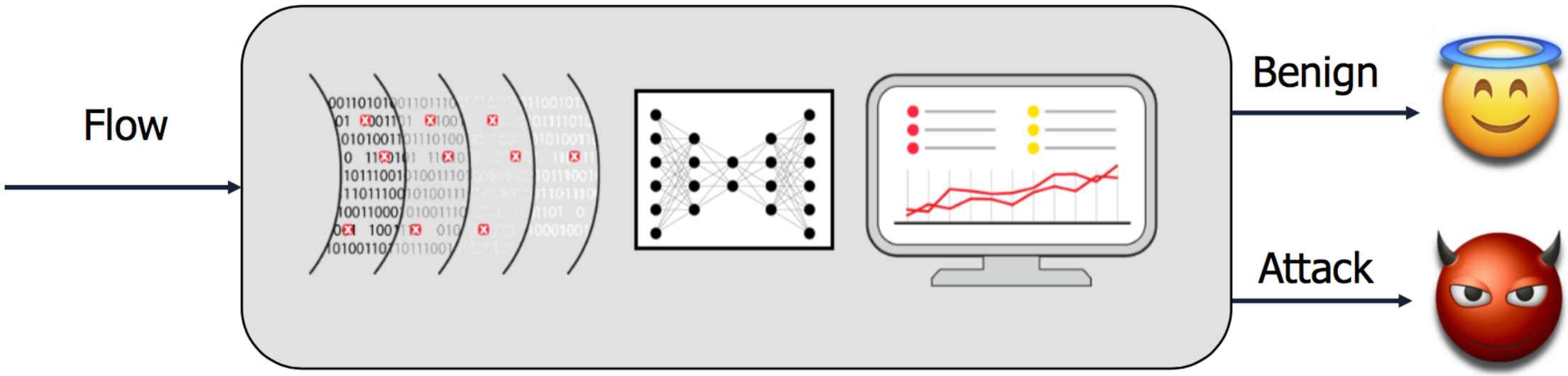


High Reconstruction Error

ALERT!

ZED-IDS

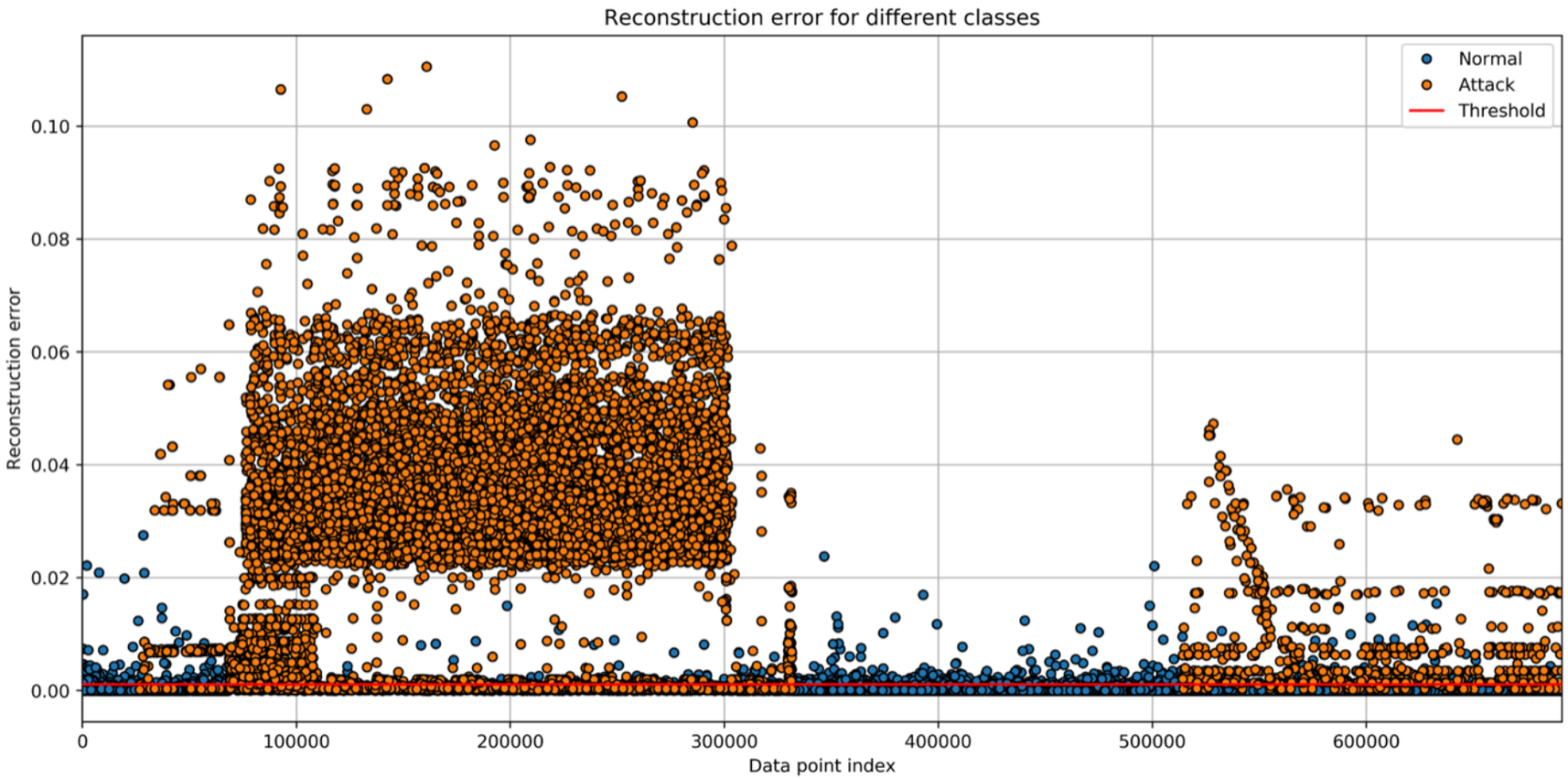
Overview

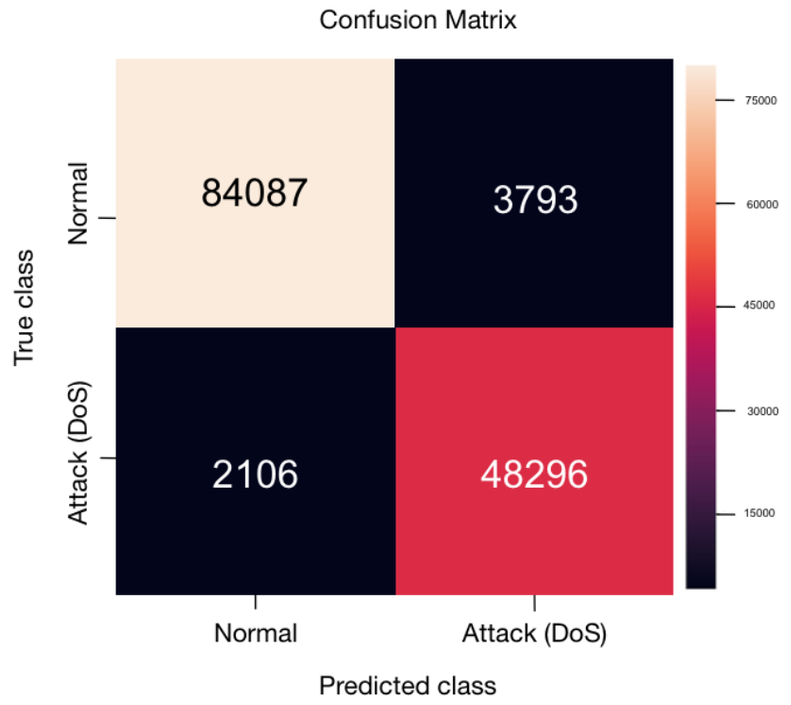


Ambiente

Risultati

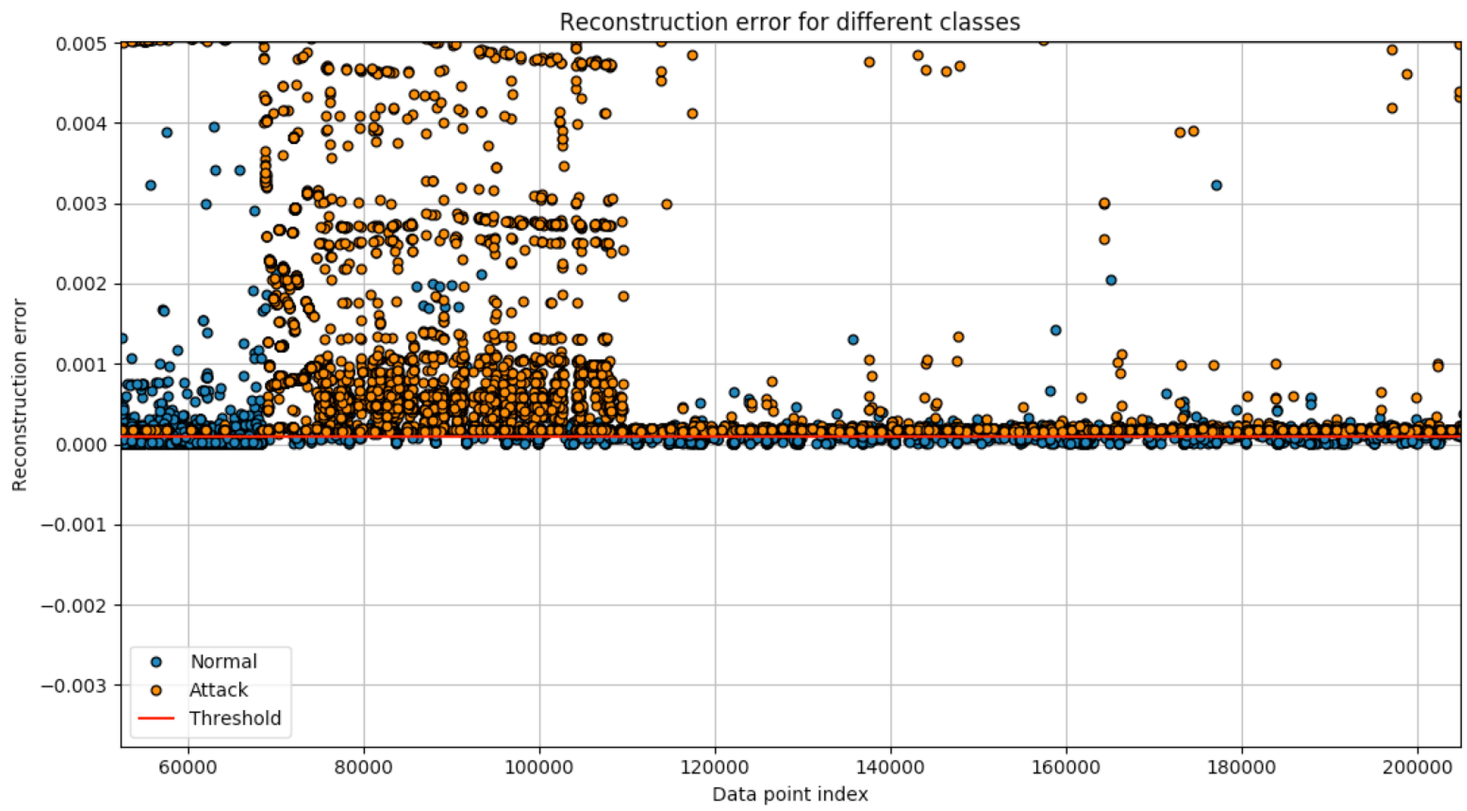
DoS-CICIDS2017





Detection Rate %	95.82
Accuracy %	95.73
False alarm rate %	4.32

zoomed plot →



Risultati-CSE-CIC-IDS2018

CICIDS2018	**Detection rate**	**False alarm rate%**
DoS Hulk	99.5	0.5
DoS GoldenEye	98.3	0.3
DoS SlowHTTPTest	98.2	1.2
DoS Slowloris	99.6	1.3
Heartbleed	98.4	0.4
PortScan	99.4	1.1
DDoS	98.3	0.9
FTP-SSH Patator	99.2	0.4
Botnet	97.4	2.2
Web Attack	98.2	0.8

Simulazione di uno 0-day

Simulazione di uno 0-day (1)

Obiettivo: riconoscere attacchi mai visti prima

Test sui DoS

Hulk trattato come uno 0-day

- training del modello senza Hulk
- comparazione con classificatori supervised

Scenario 1 - Hulk known

Learning set	Test set
DoS Hulk	**DoS Hulk**
DoS Goldeneye	DoS Goldeneye
DoS Slowloris	DoS Slowloris
DoS SlowHTTPTest	DoS SlowHTTPTest
Heartbleed	Heartbleed

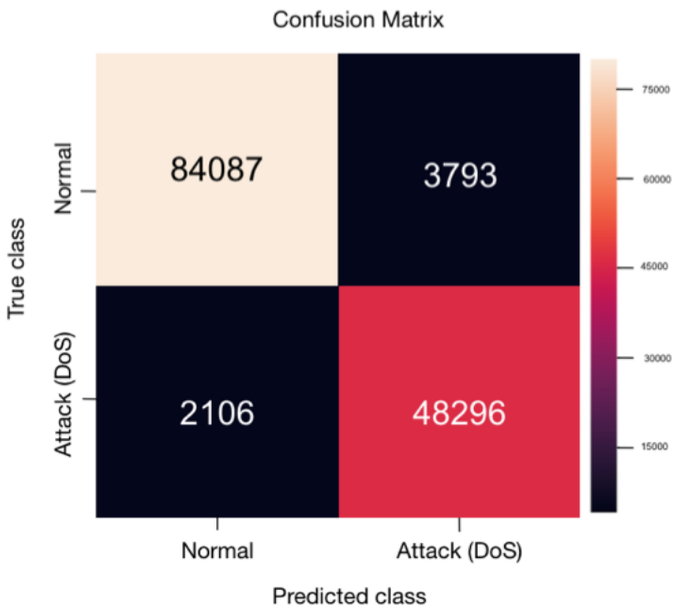
Scenario 2 - Hulk0-day

Learning set	Test set
DoS Goldeneye	**DoS Hulk**
DoS Slowloris	DoS Goldeneye
DoS SlowHTTPTest	DoS Slowloris
Heartbleed	DoS SlowHTTPTest
	Heartbleed

Simulazione di uno 0-day (2)

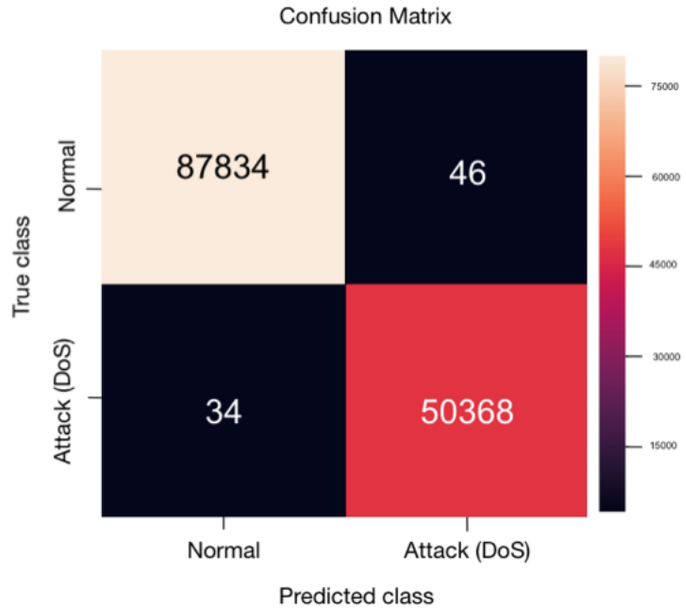
comparazione delle performance - Hulk-known

ZED-IDS



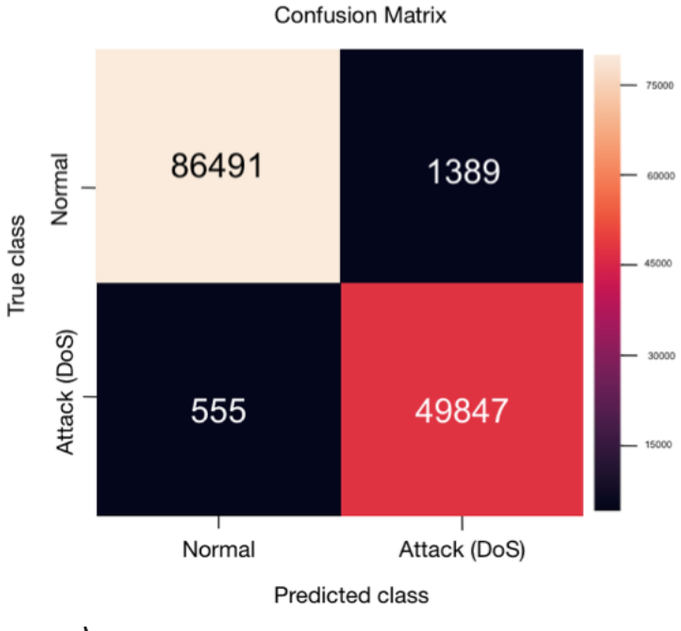
a)

Random Forest



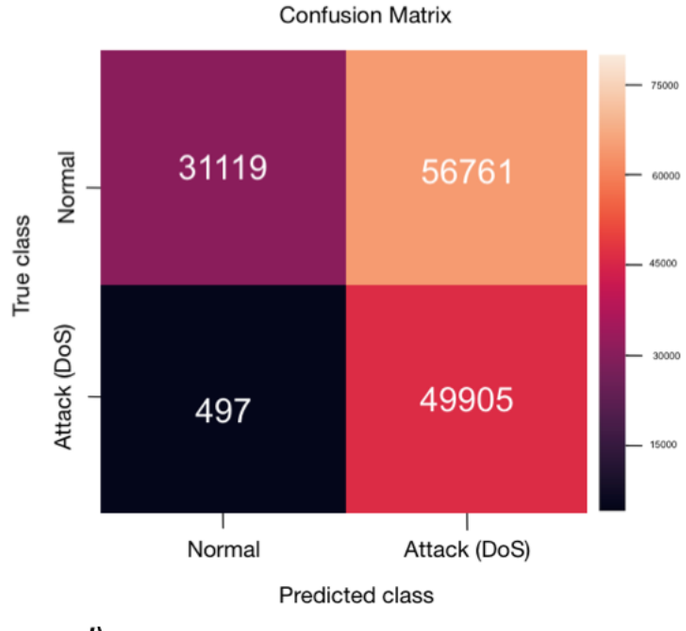
b)

QDA



c)

Naive Bayes

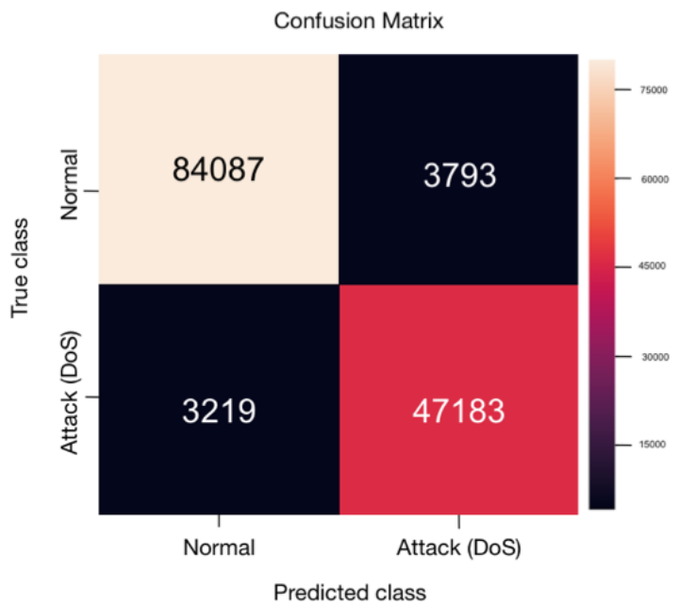


d)

Simulazione di uno 0-day (3)

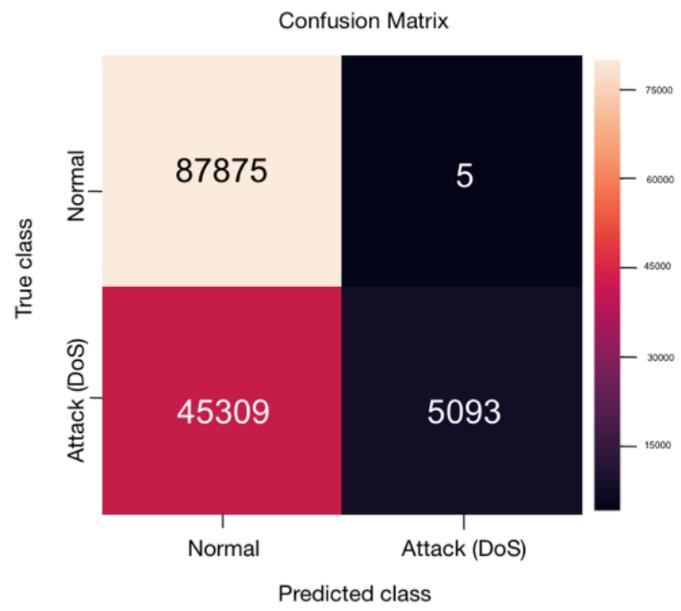
comparazione delle performance - Hulk-0day

ZED-IDS



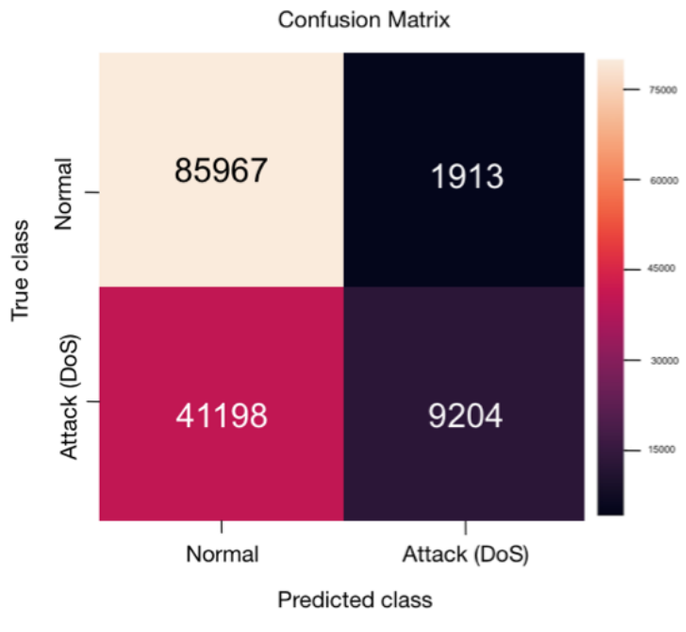
a)

Random Forest



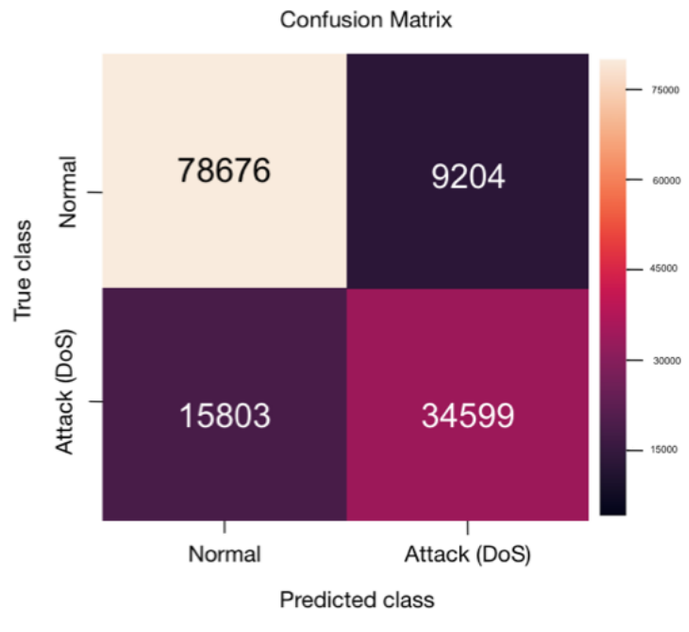
b)

QDA



c)

Naive Bayes



d)

Simulazione di uno 0-day (4)

Overview

Network/algorithm	Detection rate %		Accuracy %		Precision %		False alarm rate %	
	Hulk-known	***Hulk-0day***	***Hulk-known***	***Hulk-0day***	***Hulk-known***	***Hulk-0day***	***Hulk-known***	***Hulk-0day***
Random Forest	99.93	10.00	99.94	67.23	99.91	99.90	0.05	0.01
QDA	98.90	18.26	98.59	68.82	97.29	82.79	1.58	2.18
Naive Bayes	99.01	68.65	58.59	81.92	46.79	78.99	64.59	10.47
ZED-IDS AE	95.82	93.61	95.73	94.93	92.72	92.56	4.32	4.32

Conclusioni

- Tempi di training e di detection bassi
- Possibile integrazione in tool per la detection di attacchi real-time
- Modello potenzialmente utile per il riconoscimento di 0-day

«Change is challenging. And security is like a moving target, so make sure you are able to deal with and work through frequent changes.»

- Cindi Carter

martacatillo@gmail.com