

MARTA CATILLO

Consortium
GARR

THE ITALIAN
EDUCATION
& RESEARCH
NETWORK

A deep learning intrusion detection system



GIORNATA DI INCONTRO
BORSE DI STUDIO GARR
"ORIO CARLINI"
6 DICEMBRE 2018 ROMA

Roma, 6 Dicembre 2018

Borsisti Day 2018



Sintesi dell'attività

Obiettivo

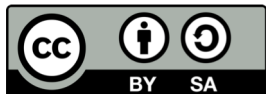
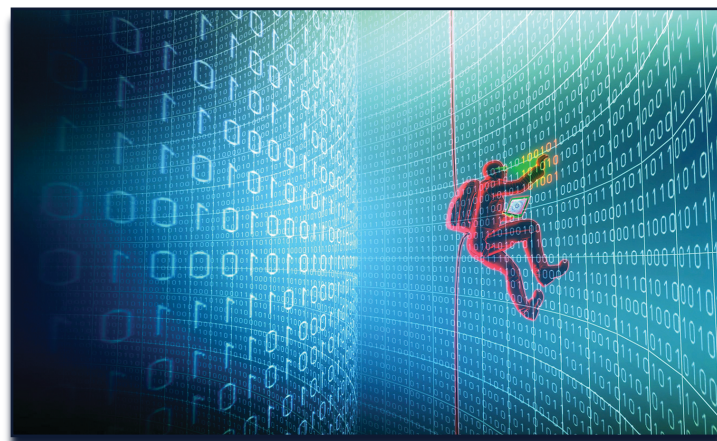
Uso di tecniche di Deep-Learning per la detection di 0-day attacks e realizzazione di un network Intrusion Detection System anomaly-based

Motivazione

Gli attuali IDS sono inefficaci per attacchi non noti

Sede

Dipartimento di Ingegneria dell'Università degli Studi del Sannio-DING





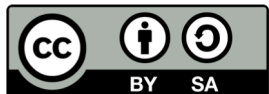
Descrizione



- NIDS anomaly-based
- Basato sull'analisi di flussi

Challenge

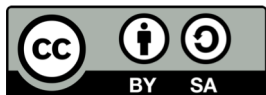
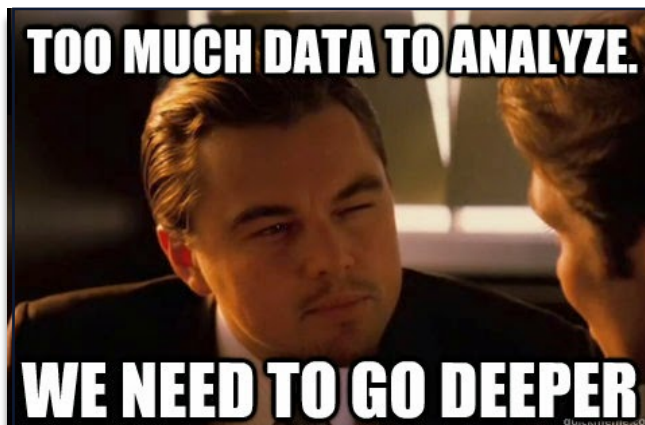
- Utilizzare tecniche di machine learning non supervisionato per la detection di attacchi non noti
- Superare i limiti che caratterizzano i classificatori basati su tecniche di machine learning supervisionato





Metodologia

- SOTA dei dataset disponibili
- Analisi dello stato dell'arte delle di tecniche di ***apprendimento non supervisionato*** per intrusion detection basate sull'analisi dei flussi di traffico normali e anomali
- Definizione e sviluppo del processo di deep learning
 - training del modello
 - testing/validazione





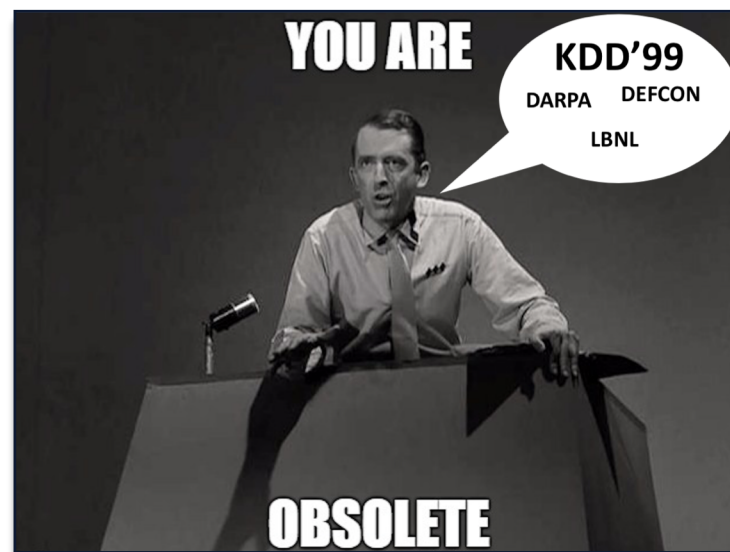
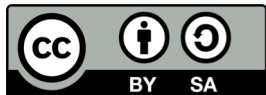
Dataset - CICIDS2017 (1)

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

Periodo di cattura

- started at 9 a.m., Monday, July 3, 2017
- ended at 5 p.m. on Friday July 7, 2017

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





Dataset - CICIDS2017 (2)

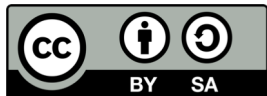
Giorno	Descrizione	Tipologia Attacco
<i>Lunedì</i>	Normal activity	
<i>Martedì</i>	Attacks + Normal Activity	BForce, SFTP, SSH
<i>Mercoledì</i>	Attacks + Normal Activity	DoS, Heartbleed
<i>Giovedì</i>	Attacks + Normal Activity	Web and Infiltration attacks
<i>Venerdì</i>	Attacks + Normal Activity	Botnet,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

Formato del dataset:

- File **pcap** per ogni singola giornata
- File **csv** contenenti flussi labelizzati creati con un generatore

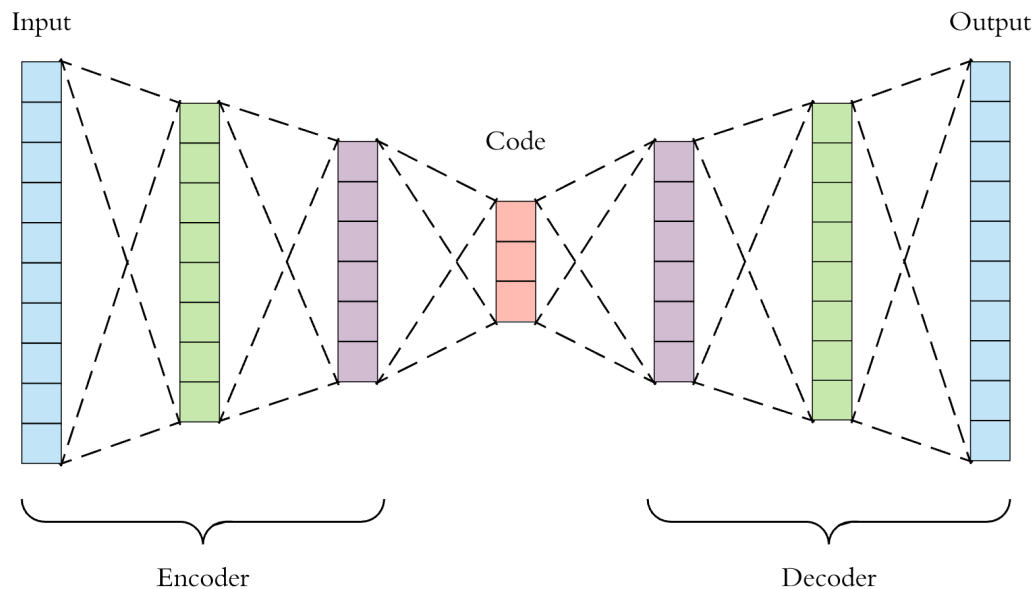
CICFlowMeter

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





Tecnica di apprendimento (1)



Autoencoder

deep neural network utilizzate per la compressione dei dati

- **Layer di encoding:** i dati di input sono compressi fino ad arrivare al collo di bottiglia
- **Layer di decoding:** i dati sono decompressi



Tecnica di apprendimento (2)

- **Encoder**

mappa deterministica f_{θ} che trasforma un vettore input x in una sua rappresentazione y

- **Decoder**

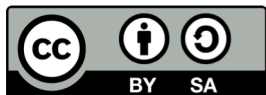
funzione g_{θ} che mappa all'indietro la rappresentazione y fino all'input ricostruito z

Il training di questa rete procede per minimizzazioni successive dell'errore di ricostruzione (**RE**) commesso da z nell'approssimare x .

$$L(x, x') \approx ||x - x'||^2$$

Reconstruction Error

RE = mean squared distance
tra input e output



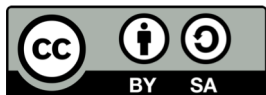


Ambiente di sviluppo

Keras (Tensorflow backend)



- **Tensorflow:** libreria open-source per machine learning sviluppata dal Google Brain team
- **Keras:** libreria per reti neurali scritta in Python

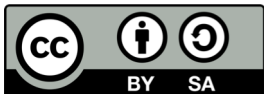




Training modello

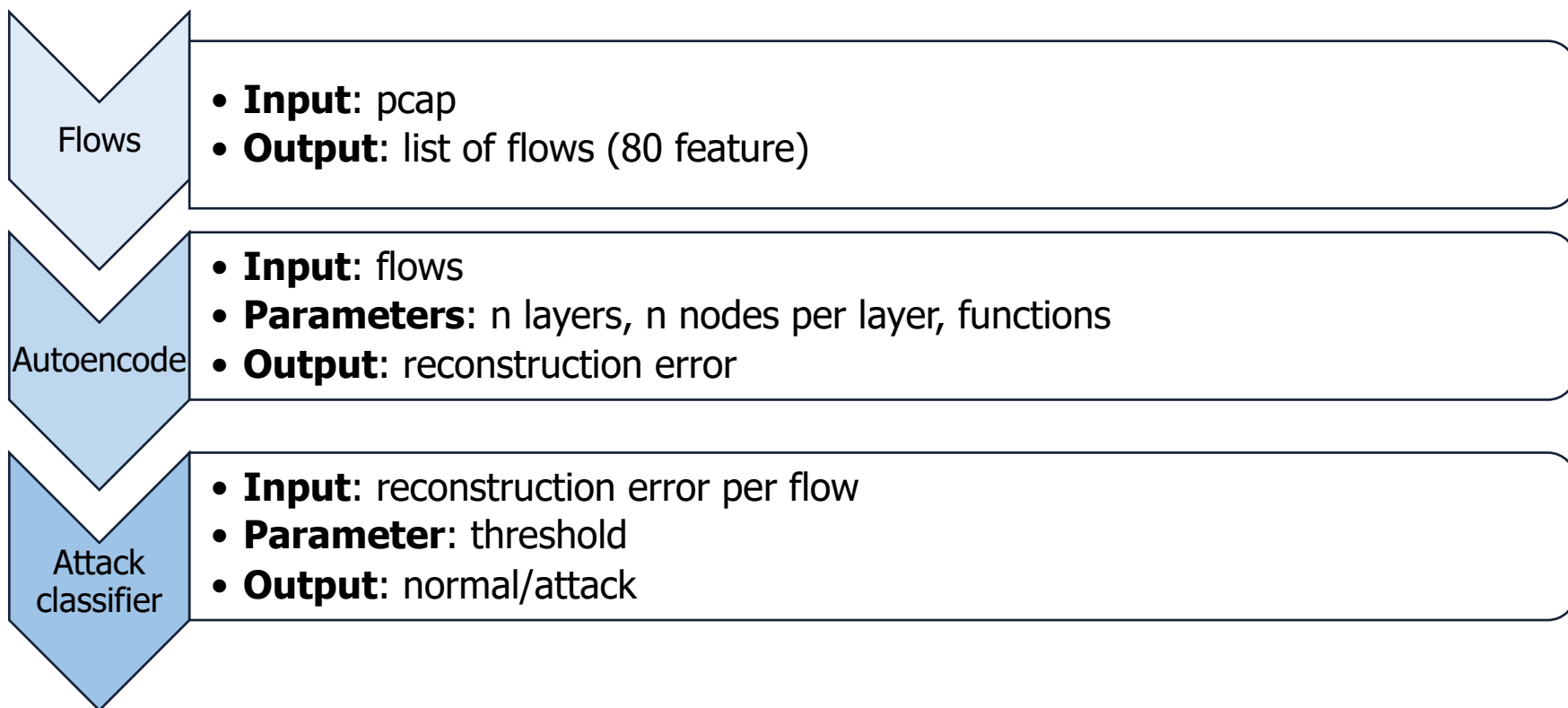
Autoencoder: learning

- **How:** minimize reconstruction error (mean square distance)
- **Training set:** Only BENIGN
- **Optimization:** Keras to optimize n. layers, n. nodes, functions





The Big Picture



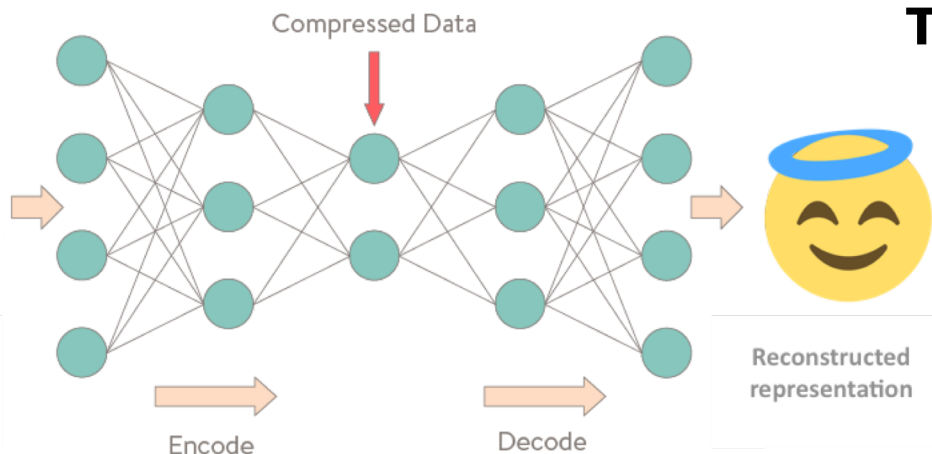


Analisi del traffico

Test set: BENIGN + ATTACKS



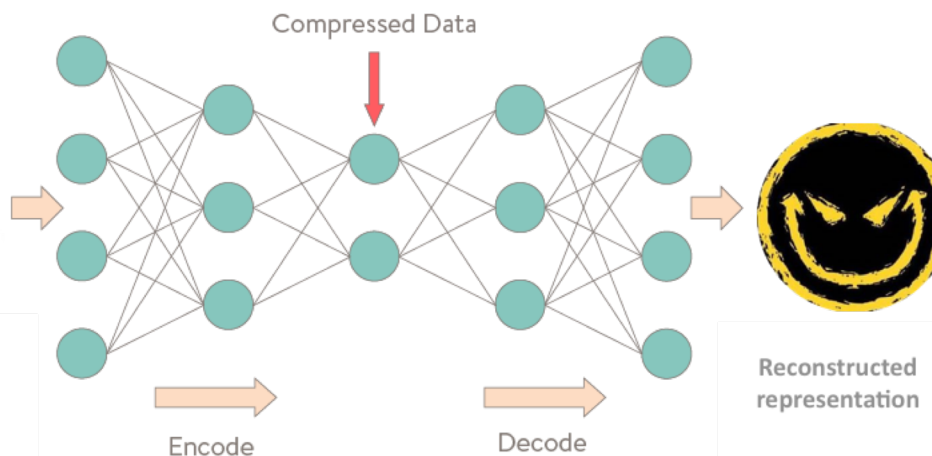
Benign



Low Reconstruction Error

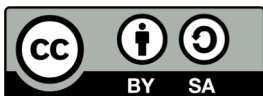


Attack



High Reconstruction Error

ALERT!!!





Test preliminari (DoS)





Set di Dati

File **csv** del Mercoledì: attacchi DoS + normal activity

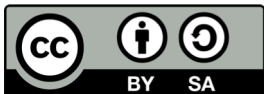
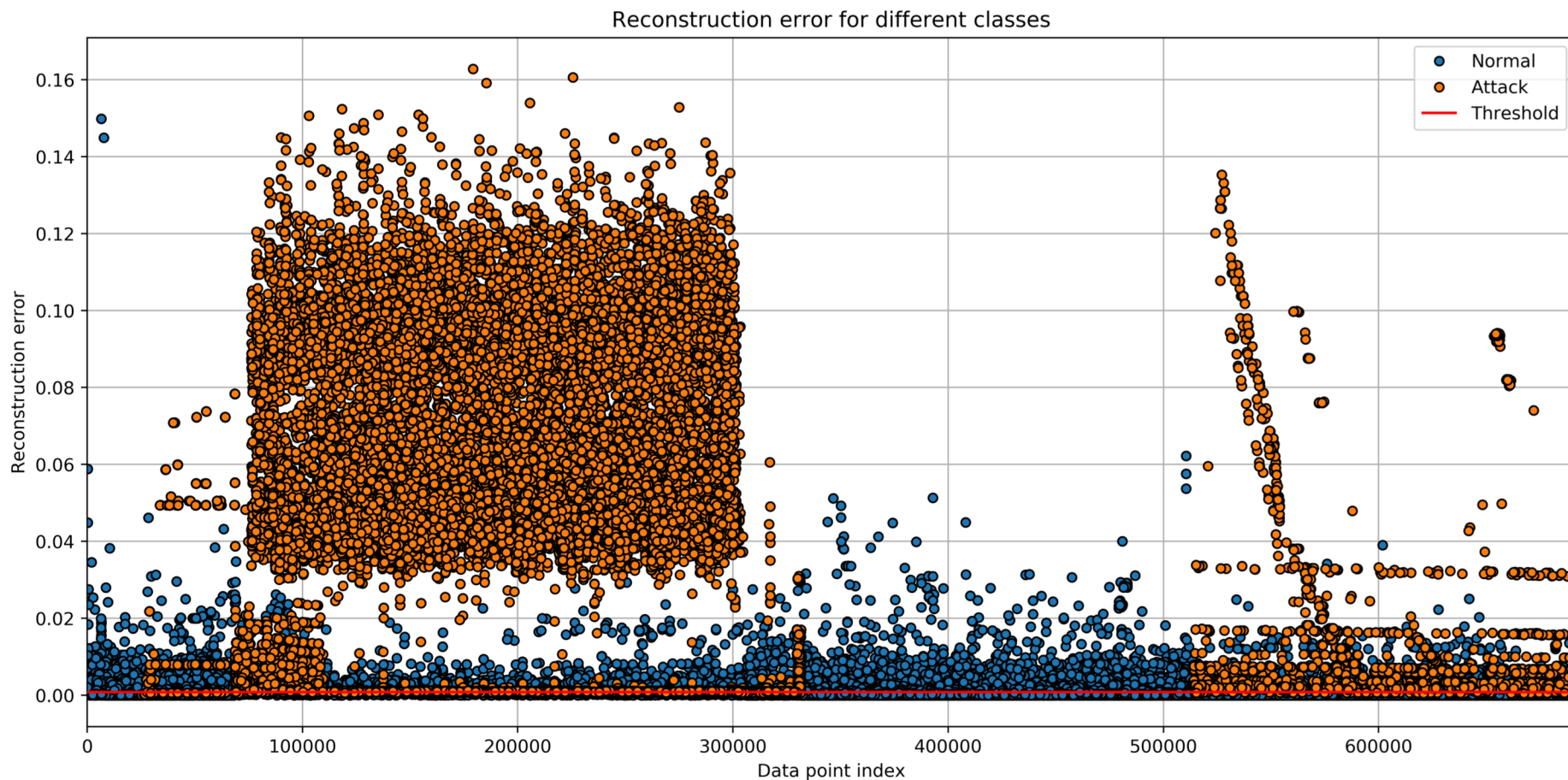
Attacchi



DoS Slowloris
DoS Slowhttptest
DoS Hulk
DoS Goldeneye

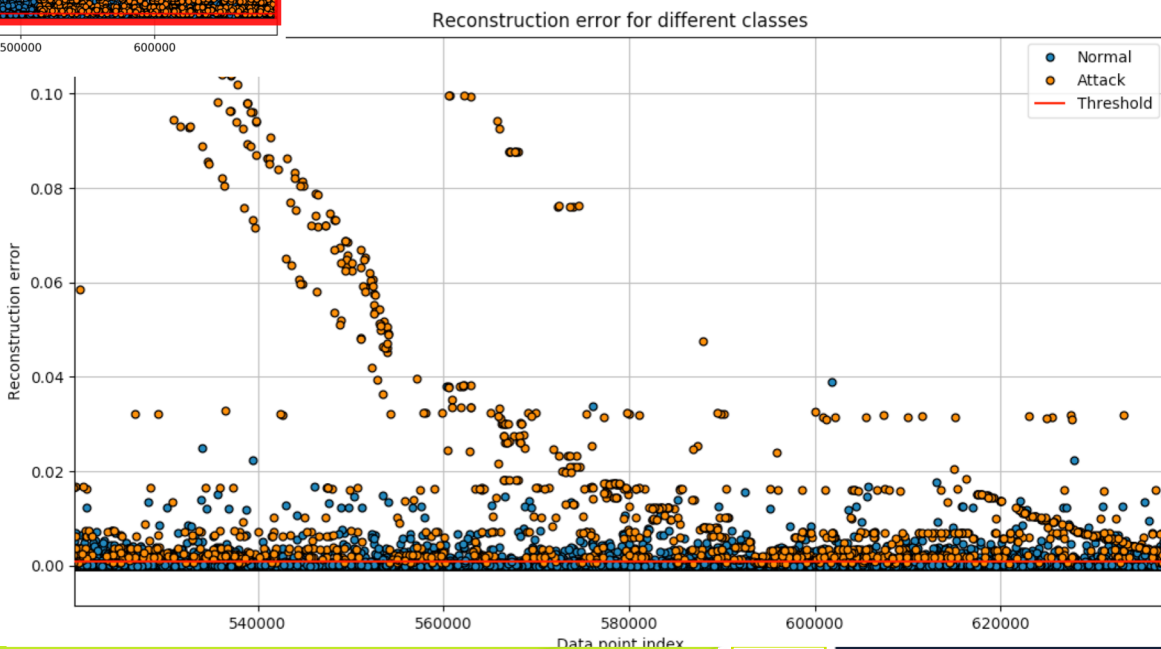


Reconstruction Error - traffico del Mercoledì (BENIGN + ATTACK)



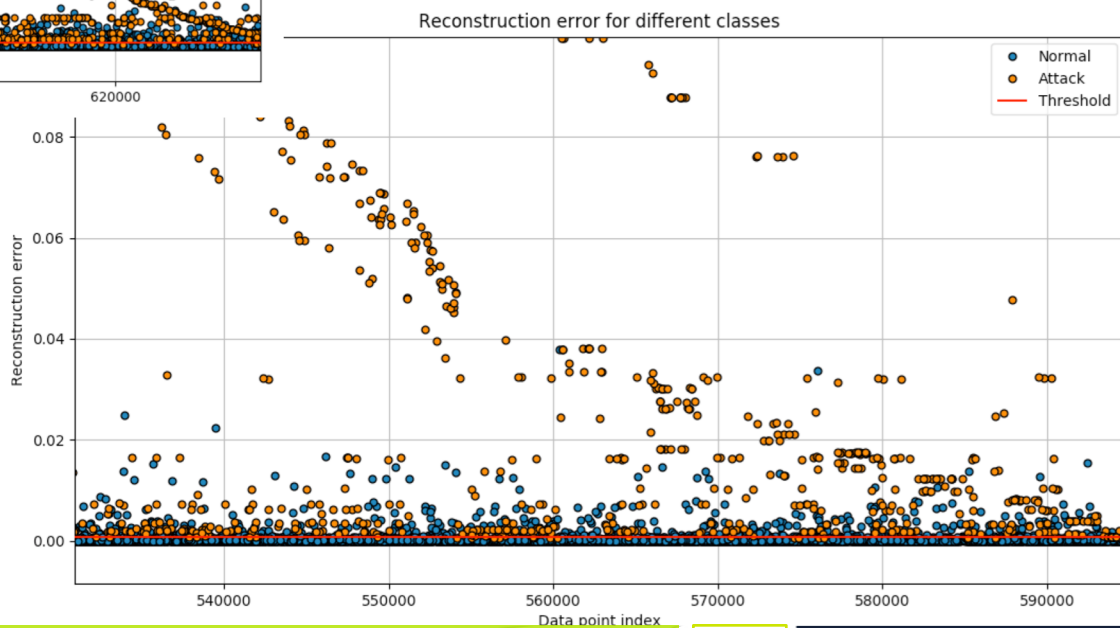


Reconstruction Error – zoomed plots (1)



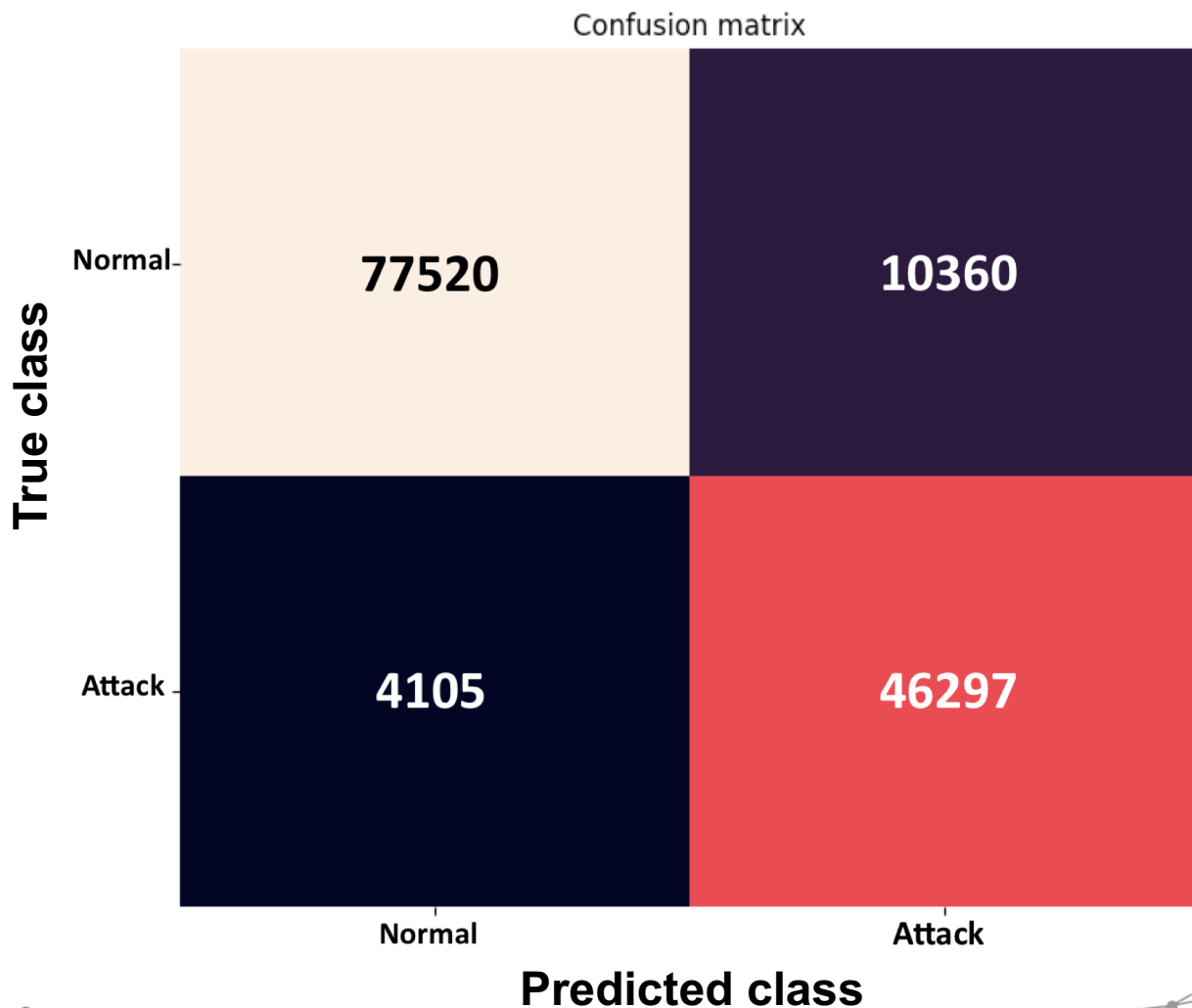


Reconstruction Error – zoomed plots (2)





Valutazione (1)





Valutazione (2)

False positive rate FPR

$$FPR = \frac{FP}{FP+TN} = 0.12$$

False negative rate FNR

$$FNR = \frac{FN}{FN+TP} = 0.081$$

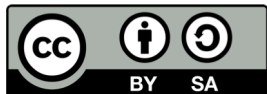
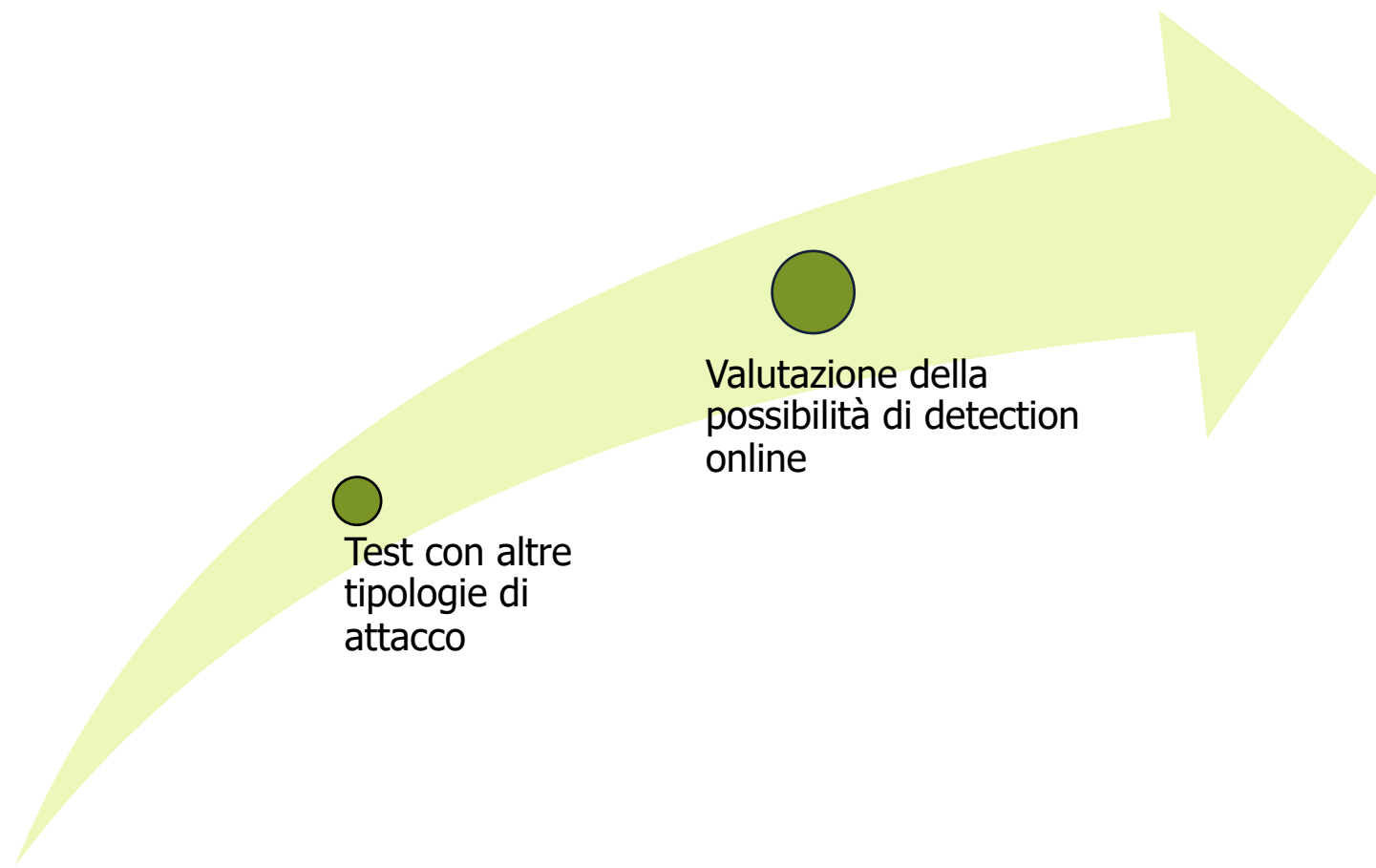
Detection rate: 91.86%

False alarm rate: 11.79%





Sviluppi futuri - secondo/terzo trimestre





Lust for victory will not give you the victory. You must receive the victory from your opponent. He has no choice but to give it to you because he will sense your heart as better or truer. Nature is your friend; it helps you to win. Your enemy will have unnatural movement; therefore you will be able to know what he is going to do before he does it.



Masaaki Hatsumi

Secret Ninjutsu

Marta Catillo
martacatillo@gmail.com

