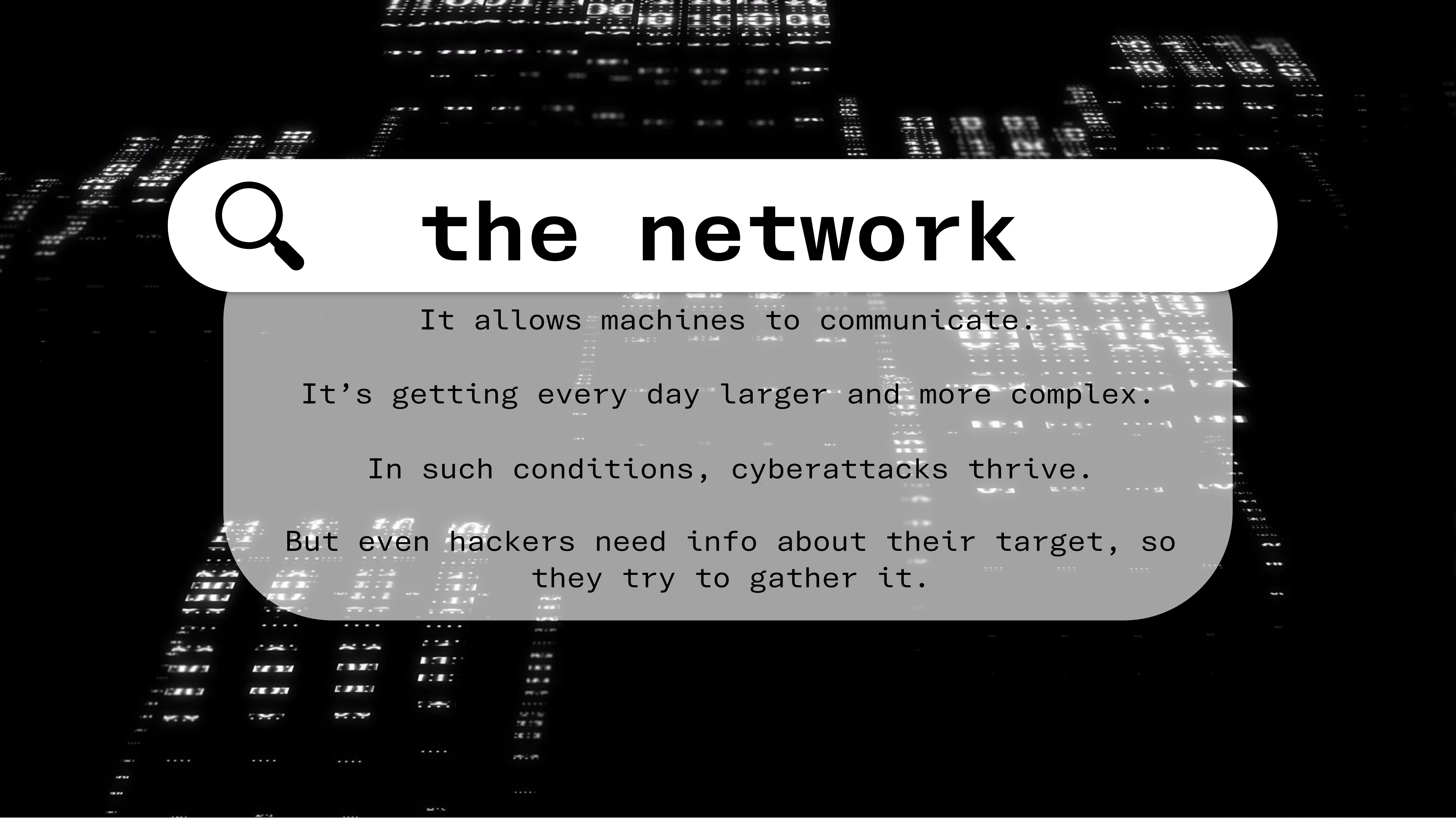
Detecting Recon Attacks on IoT Devices

// Domenico Fumagalli



the network

It allows machines to communicate.

It’s getting every day larger and more complex.

In such conditions, cyberattacks thrive.

But even hackers need info about their target, so they try to gather it.

This is called reconnaissance : accessing the network information necessary to perform an attack.

This kind of attack is very quiet and hard to detect.

Can we use Machine Learning to detect them?

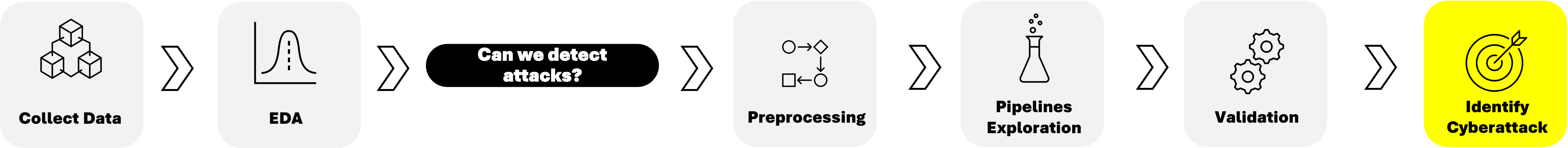
To do this we would need labeled data about the attacks. This kind of data is very hard to get.

For this reason, University of New Brunswick (UNB) ran a cybersecurity experiment designed to generate such data.

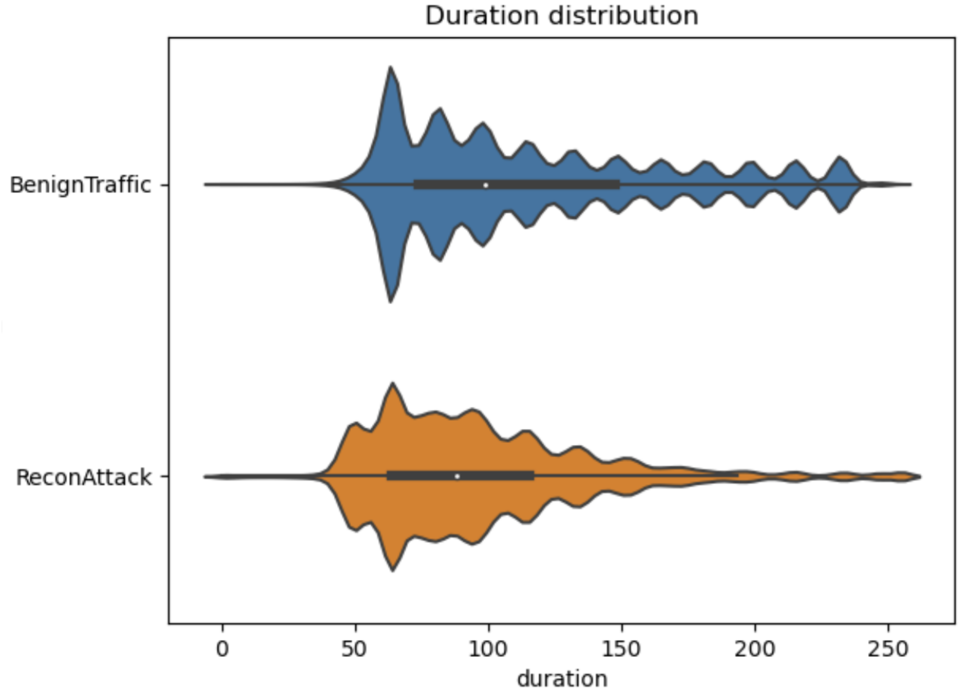
The researchers used real cyberattack tactics and tools on a large smart home setup.

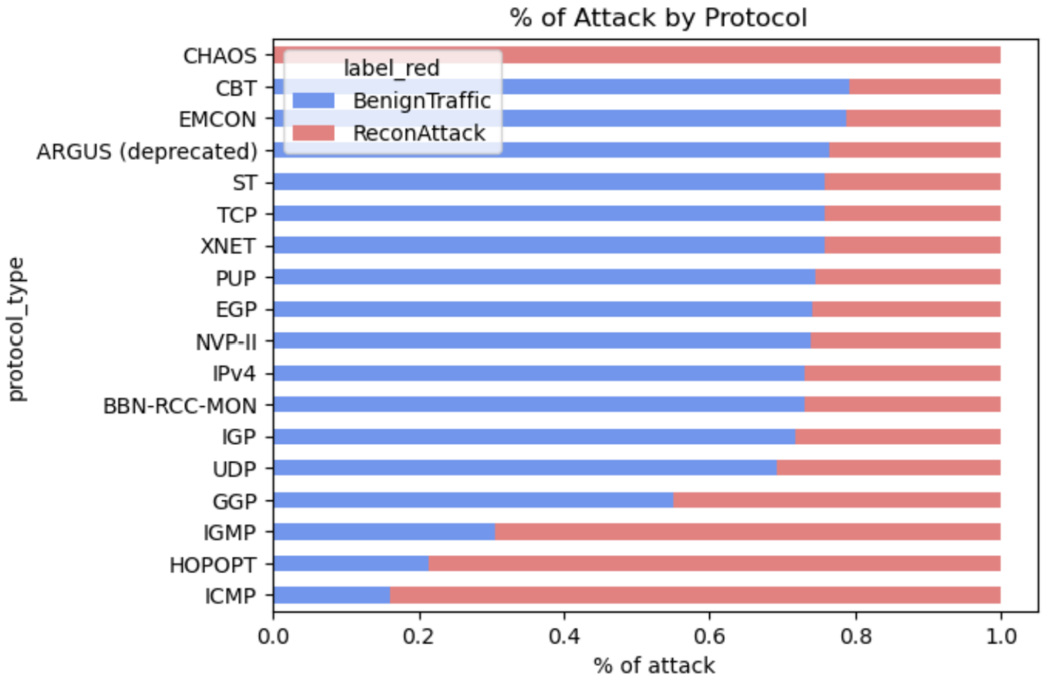
By focusing only on recon cyberattacks my first objective was to develop a reliable model that could identify them.

To do so I relied on the classic data science process flow.



Although there was a difference in the network data, most of cyberattacks are indeed sneaky.

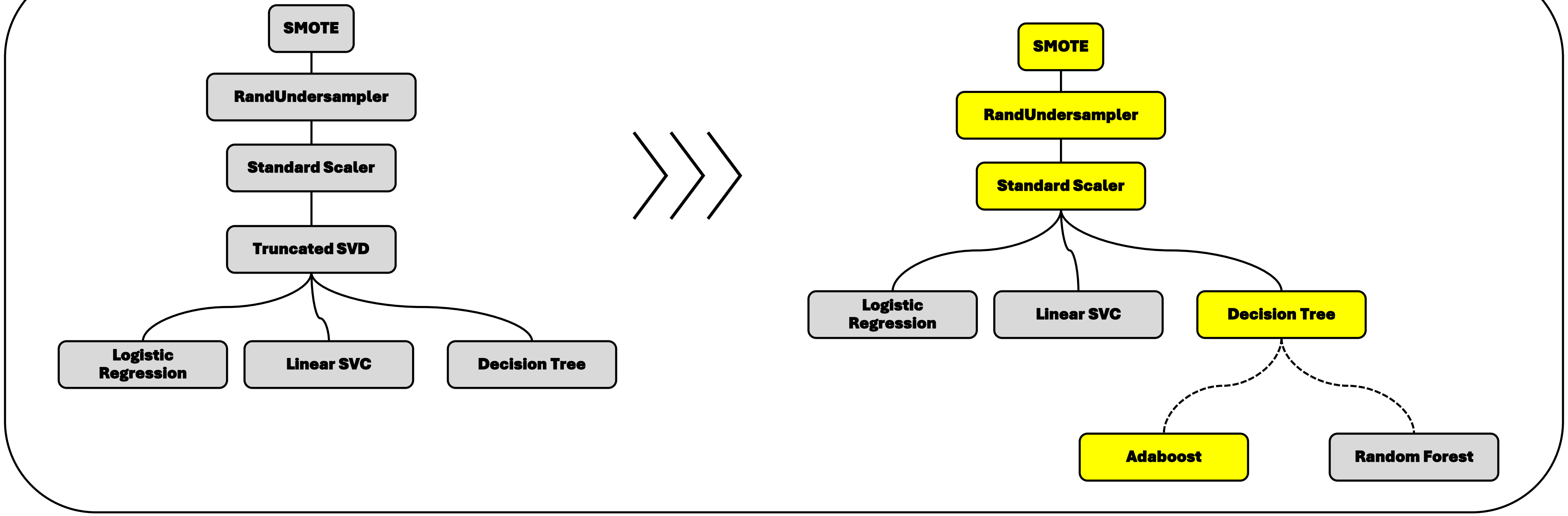




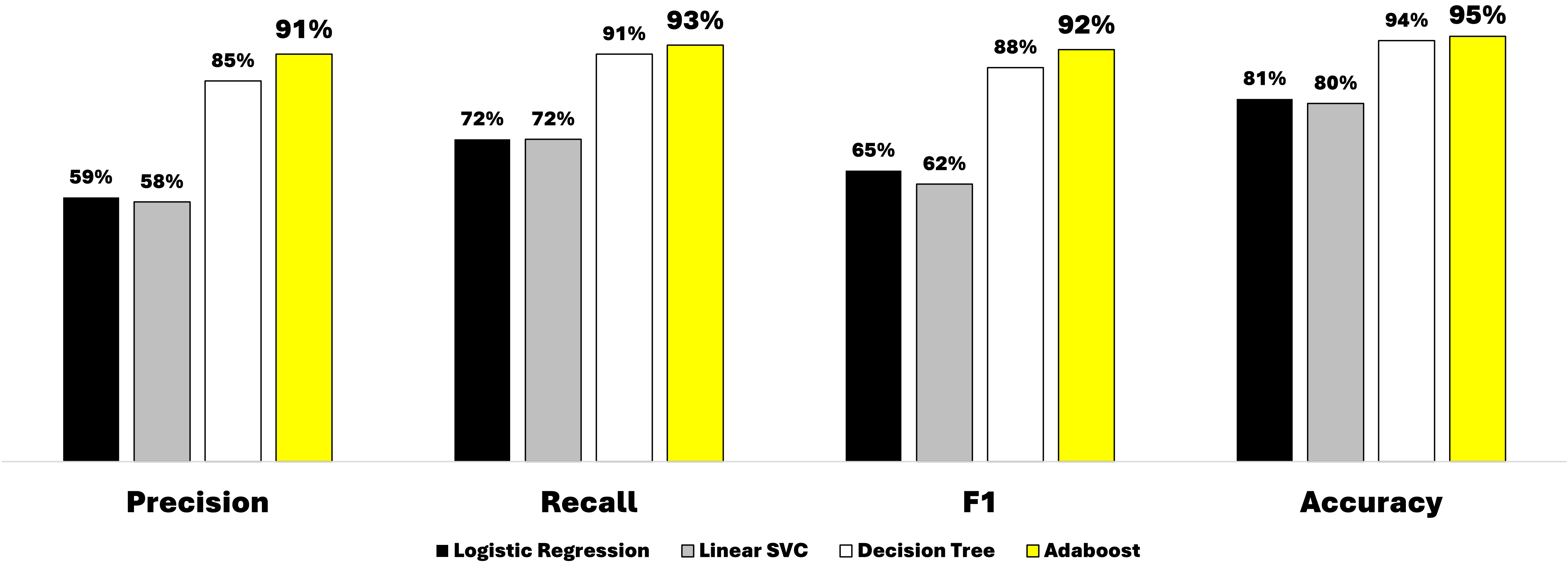
After multiple iteration I did learn that the best models where threshold-based models, the family of decision trees.

Working in pipelines and using cross validation was key to find the best options.

Pipeline evolution example

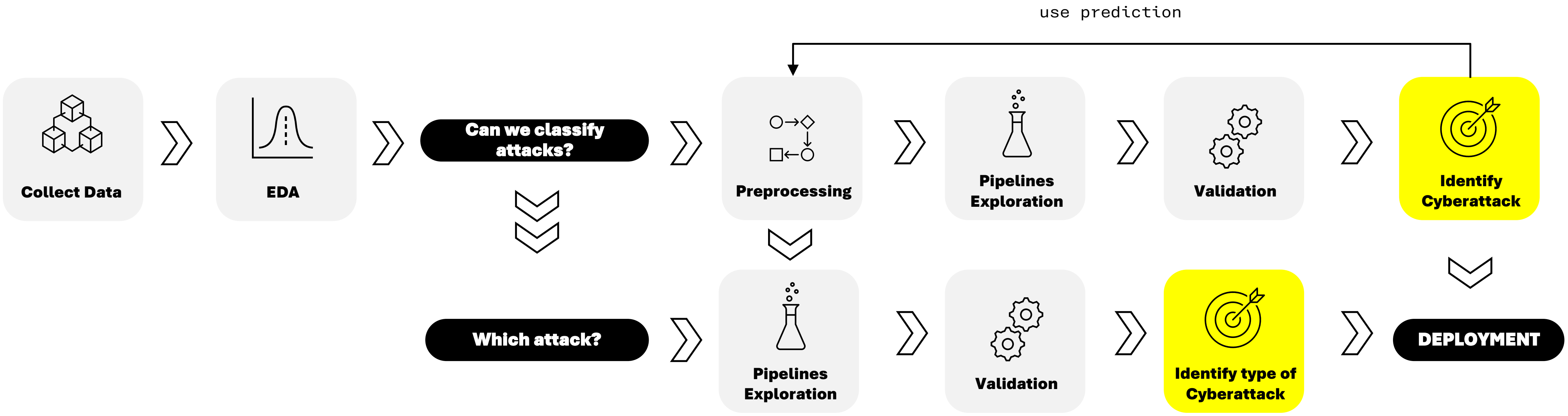


I did find success with Adaboost built on top of an optimized decision tree.

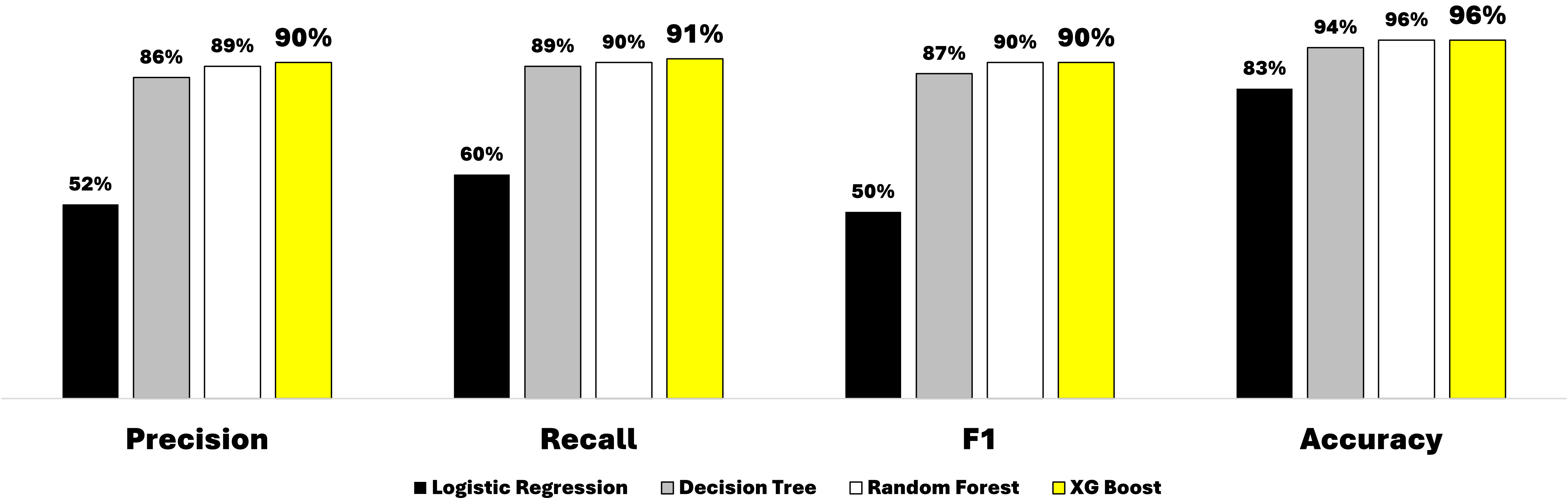


But can we also detect the kind of recon attack occuring?

After having a great model in the binary classification I employed adaboost’s prediction as a feature on which to train the multiclass classifiers.



In this task Random Forest and XG Boost performed very well. However XG Boost generalized better, predicted faster and had slightly better recall.



Conclusion : leveraging UNB research we were able to detect reconnaissance activities from the network traffic.

We were able to demonstrate that by specializing models on the kind of cyberattacks can yield promising results.