Leveraging Machine Learning to Mitigate Phishing and Malware

Roberto Sponchioni

Manager, Threat Engineering and Detection

DocuSign

Leveraging Machine Learning to mitigate Phishing and Malware

Roberto Sponchioni

Manager, Threat Engineering and Detection, DocuSign

Agenda

- Who am I
- Why Pescatore
- Pescatore Architecture
- Challenges
- Pescatore in numbers…
- Conclusion / Takeaways

Who am I?

- Threat Engineering and Detection Manager @DocuSign
- Former Senior Anti-Malware Engineer @Symantec
- Former Security Consultant (PT/VA, Incident Response)

Contacts:

- Twitter @Ptr32Void
- Roberto.Sponchioni@docusign.com

DocuSign

The business need

Bought URL Classification System - SaaS

We bought a URL Classification system and we were submitting about 500 URLS per month

2015

2016

Increased number of URLs

# of URLs being submitted increased to 6000 per month

Internal discussion

About 9000 URLs per month. The price would have increased dramatically and the vendor was not super accurate. We decided to build it internally.

Jan 2017

Feb 2017

Development started

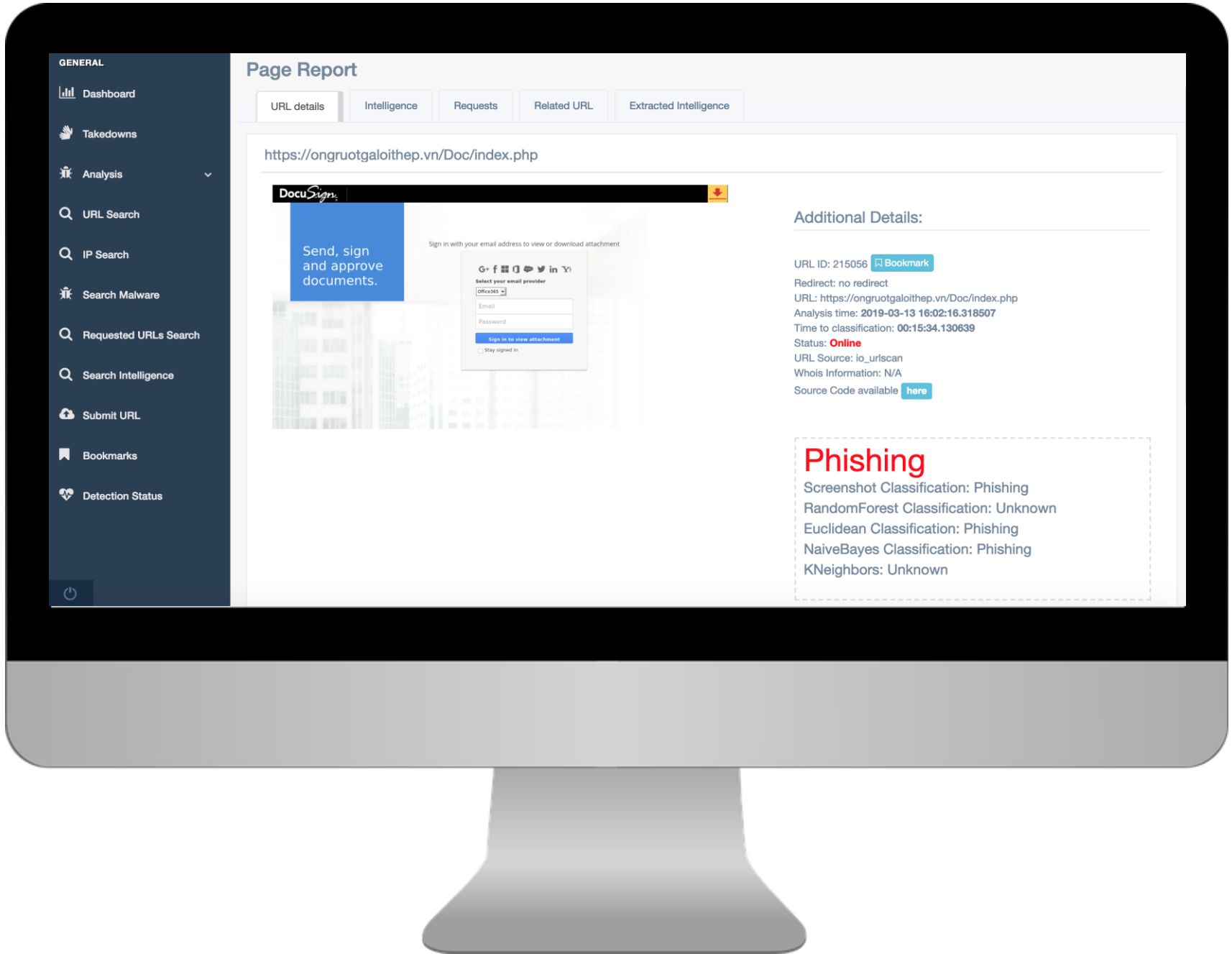
Initial development started

Started saving money

After 5 months of testing without issues, we released the project!

End of 2017

Pescatore Architecture – Front-End



Pescatore Architecture – Back-End

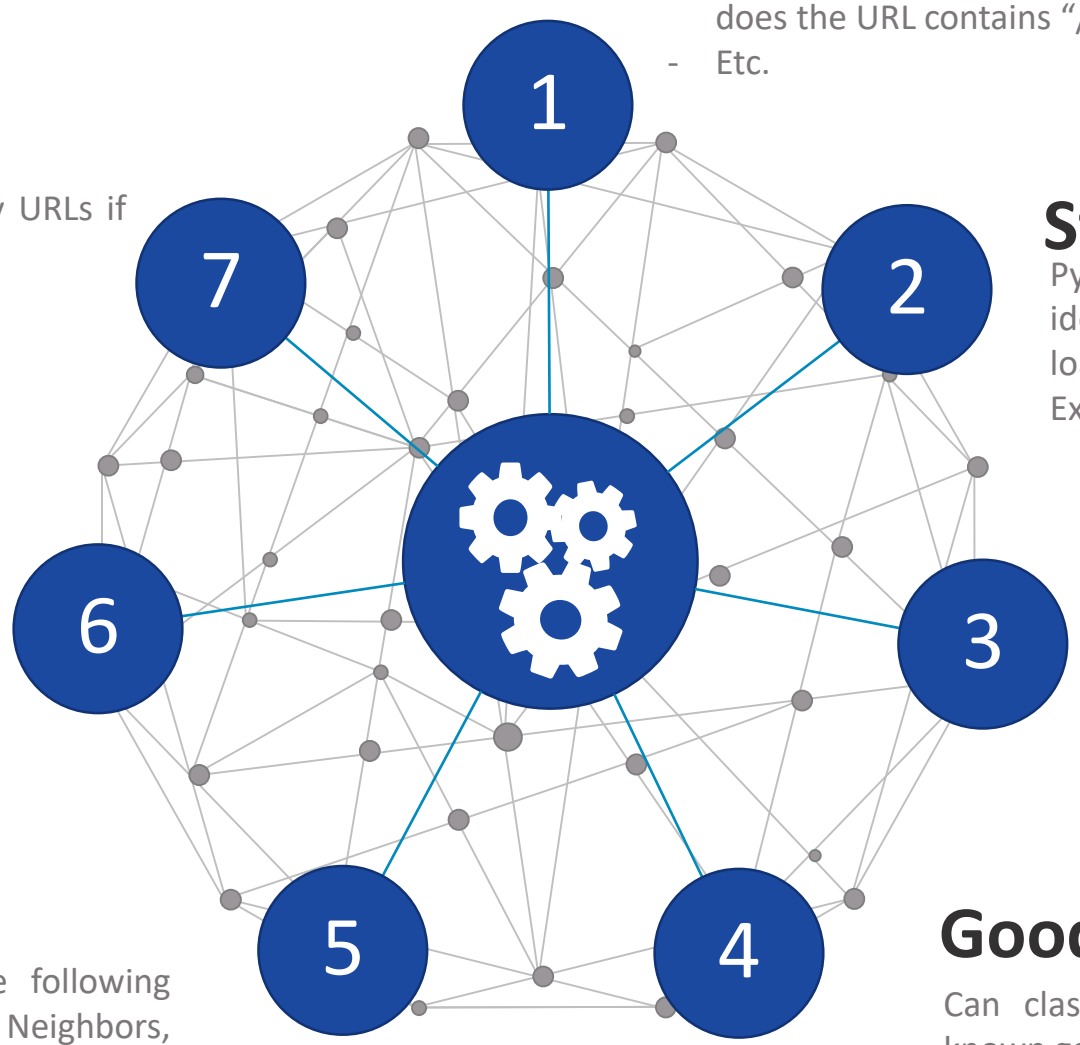
DB Heuristic

DB Heuristic classifications can classify URLs based on extracted features; for example:

- Is the URL reachable?
- Does the requested page contain login forms, a password box and does the URL contains “/wp-content” or “/images”?
- Etc.

Yara Rules

Yara rules can be used to classify URLs if Yara risk >= 100



Static Classification

Python code can be written in order to identify specific URLs that cannot be loaded using the headless browser (eg.: Exploit kits).

Naive Bayes

Naive Bayes classifier uses specific features extracted from the requests and responses that the headless browser makes

Bad Reputation

Can classify URLs based on Bad Reputation

RF, KNN, Euclidean, ScreenShot

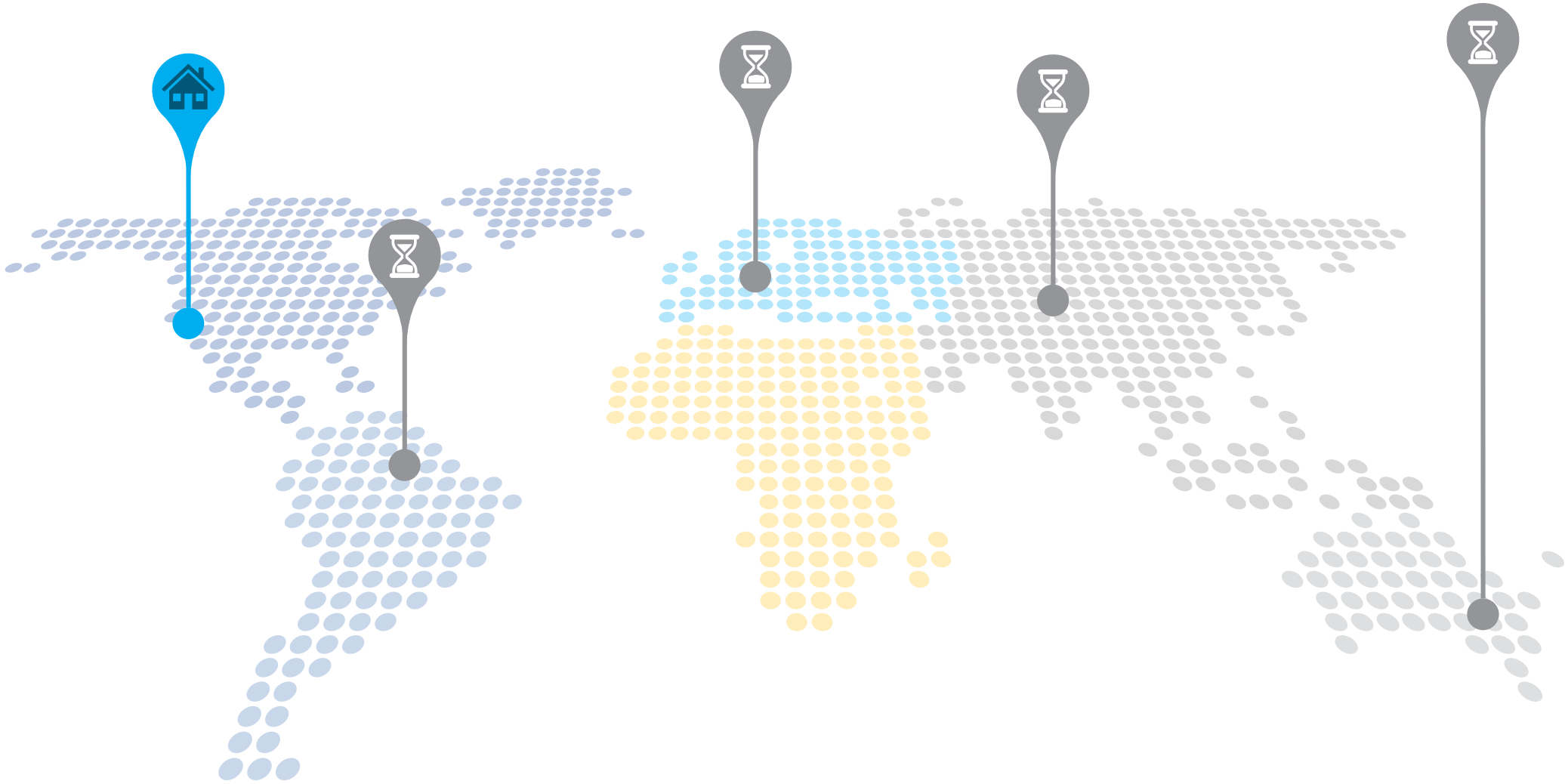
ML classification is performed using the following algorithms RandomForest, K-Nearest Neighbors, Euclidean & Screenshot

Good Reputation

Can classify URLs based on known good domains

DocuSign

Pescatore Architecture – Deploy it everywhere



Pescatore Architecture – Overall Architecture (1)

Push & Analyze

We collect URLs and we push them to Pescatore for analysis.

Classification

Pescatore classifies the URLs automatically.

Integration

Our Internal Security Orchestration and Automation system pulls the malicious URLs and stores them for later use.

Backtrace

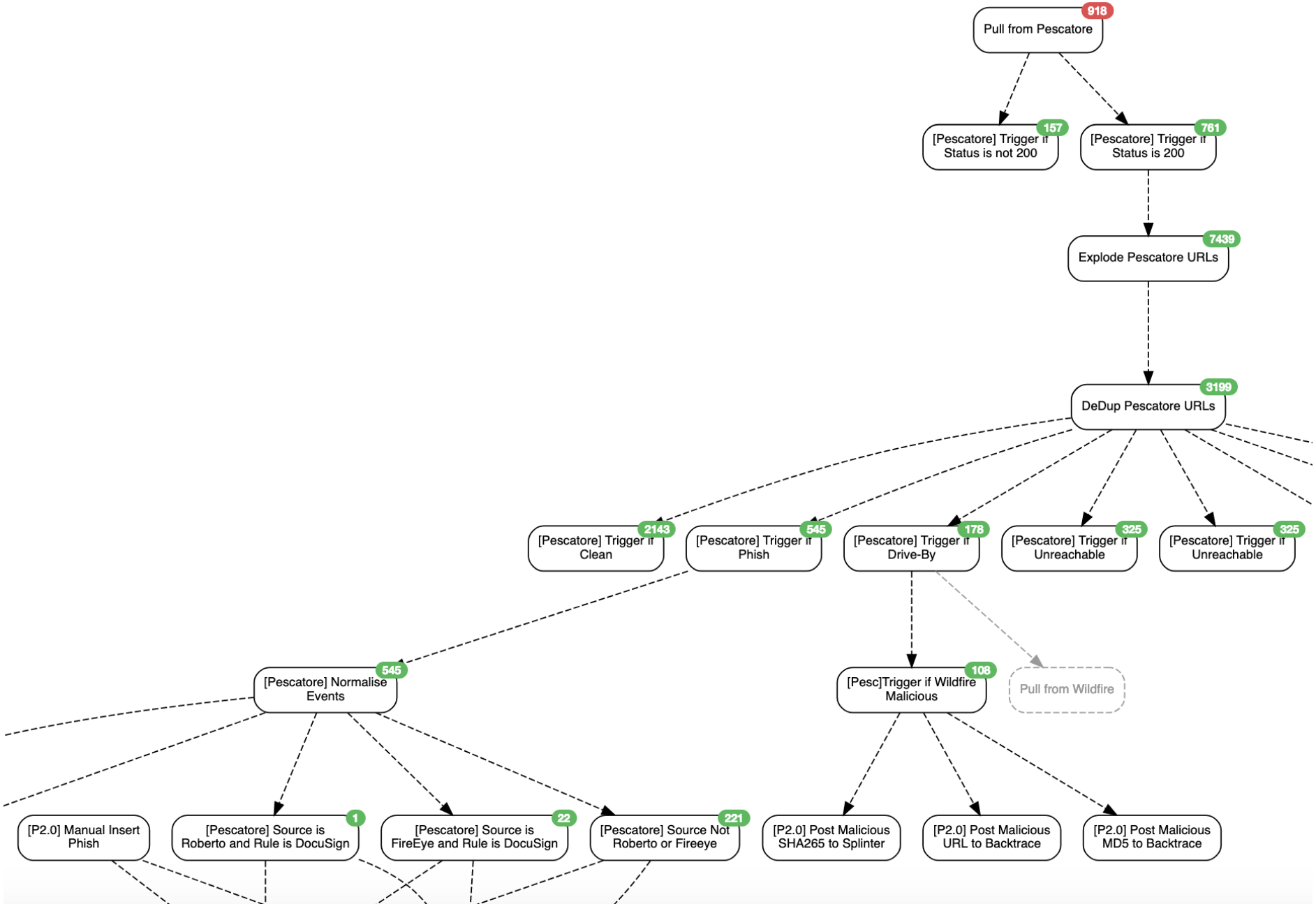
Automatically analyze logs to identify employees hitting phishing sites. If detected, we automatically:

- create incident cases
- Enrich the incident with additional details
- Email the employee

Takedowns

Specific DocuSign related phishing sites are sent for takedown.

Pescatore Architecture – Overall Architecture (2)



CHALLENGES

- Identify the features & ML algorithms (have a backup plan)
- Identify the right scalable architecture
- Do our own take downs
  - We did not know if anybody would reply to us (but they DID)
  - Partnering with Legal

Pescatore in numbers…

NUMBER OF PROCESSED URLs PER DAY

~ 550

NUMBER OF DocuSign TAKE DOWNS PER MONTH

~ 235*

* And counting…

YEARLY CLOUD PROVIDER COST

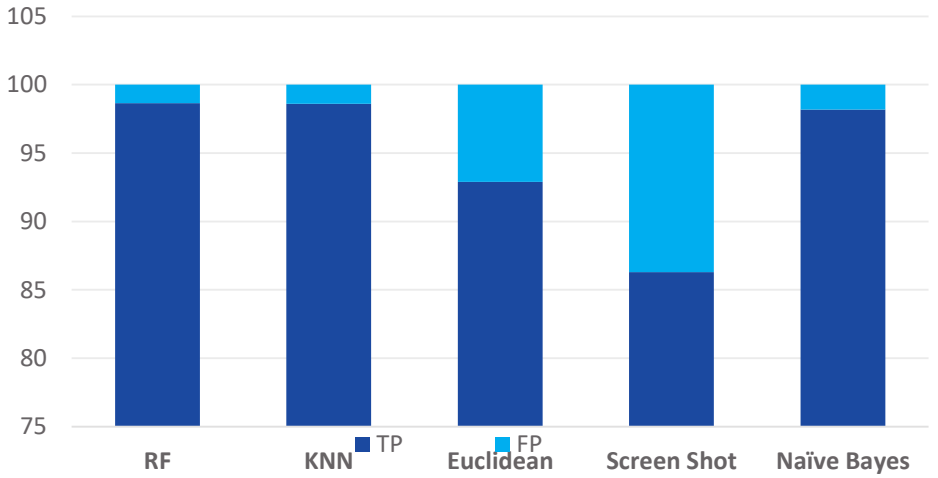
$3,600

COST CUT

~ 75%

MACHINE LEARNING TRUE POSITIVE VS FALSE POSITIVE RATE

ML	True Positive	False Positive
RF	98.66	1.34
KNN	98.60	1.40
Euclidean	92.89	7.11
Screen Shot	86.30	13.70
Naïve Bayes	98.17	1.83



AVERAGE TIME TO AUTOMATICALLY CLASSIFY A URL

6 MINS

AVERAGE TIME TO ALERT WHEN A PHISHING SITE IS HIT

3 MINS

AVERAGE TIME TO GET A SITE TAKEN DOWN

5 DAYS

DocuSign

Conclusion / Takeaways

- You want to scale, you need to automate
- Do not give up
- Do not be afraid to develop in-house tools
- Cost saving
- Do not feel you have to do everything at once, keep automating and keep developing

Thanks