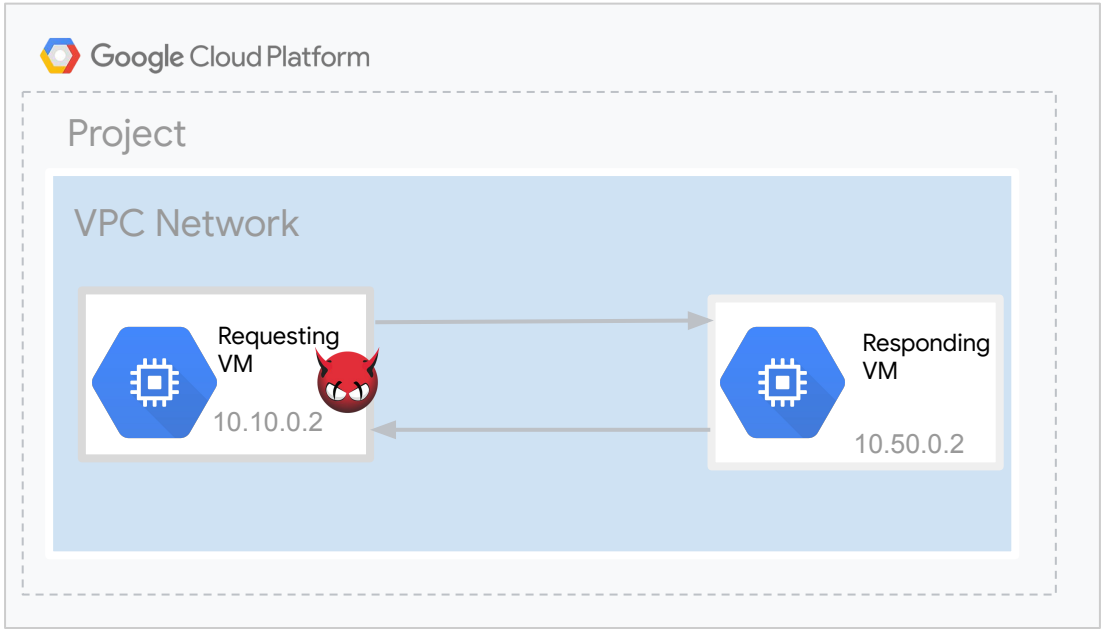
DZ220-Know Yourself, Know Your Enemy: Detecting Anomalous Behavior Using Machine Learning

Speaker: Bushra AlAhmadi
University of Oxford
@BushraAlahmadi

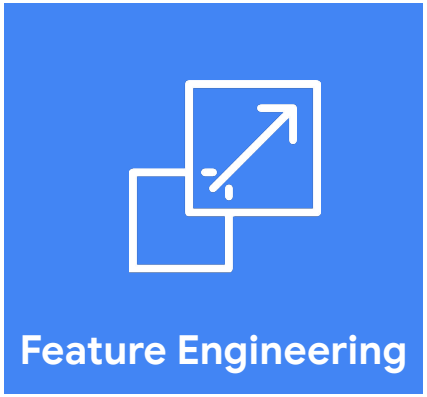
Google Cloud

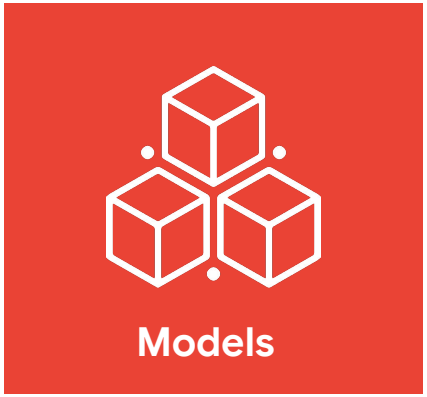
How can we detect malware on a VM?



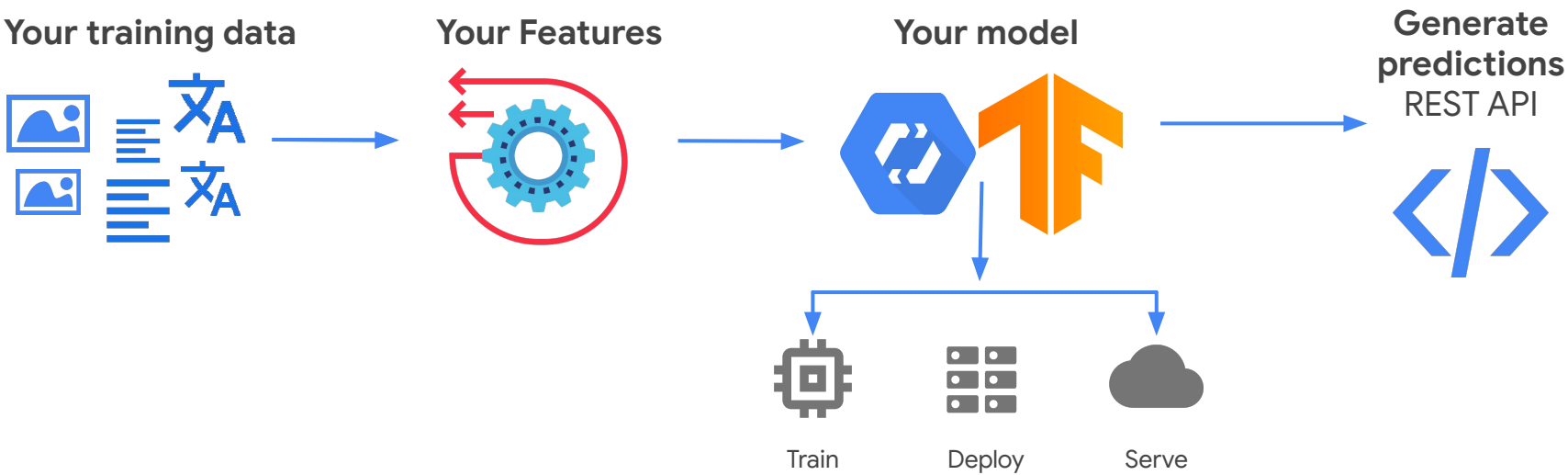
Google Cloud

Machine Learning Building Blocks





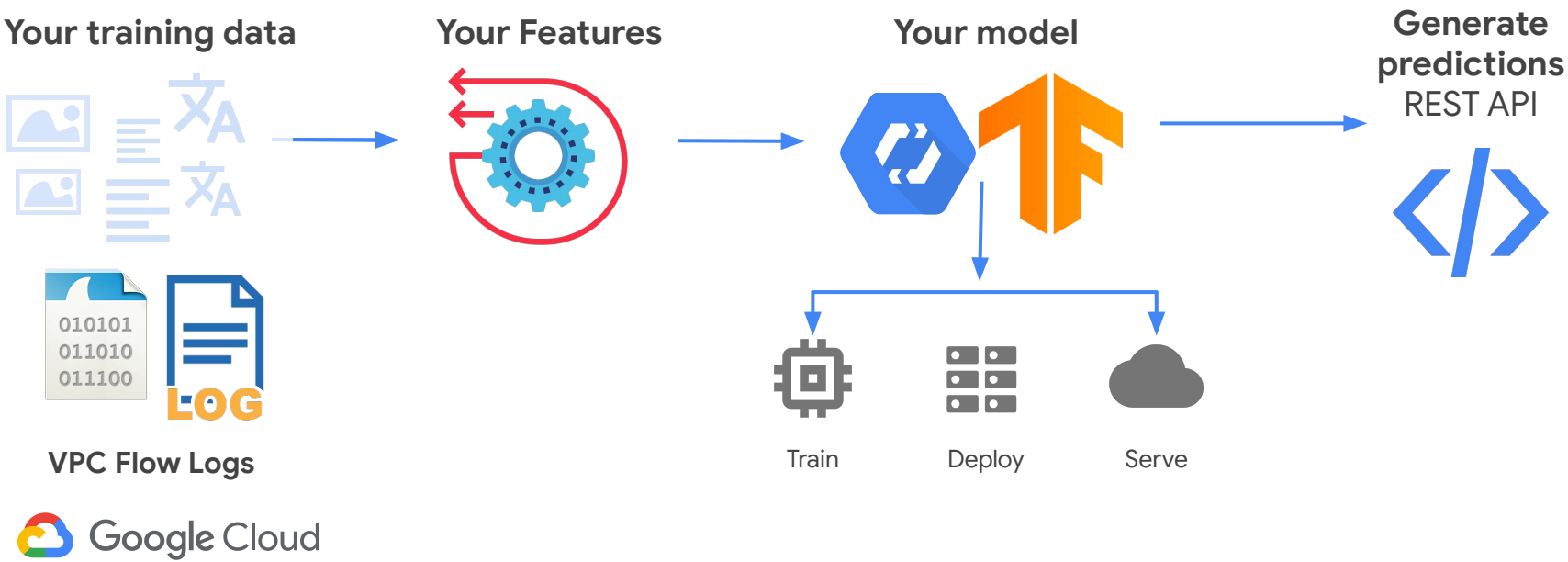
Machine Learning Process



Google Cloud

Machine Learning Building Blocks

Machine Learning Process

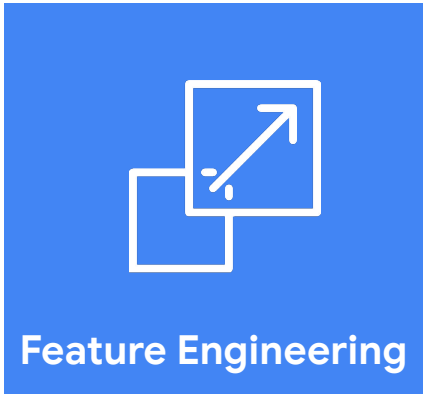


Google Cloud

Data

- Lack of labeled samples and certainty in ground truth.
- Privacy - encrypted traffic.
- Not enough or low quality data.
- Imbalanced data.
- Biased data.
- Dirty data: Garbage In -> Garbage Out.
- Missing data (i.e. due to misconfigurations).

Machine Learning Building Blocks



IS THIS A

CAT or DOG?

CAT DOG

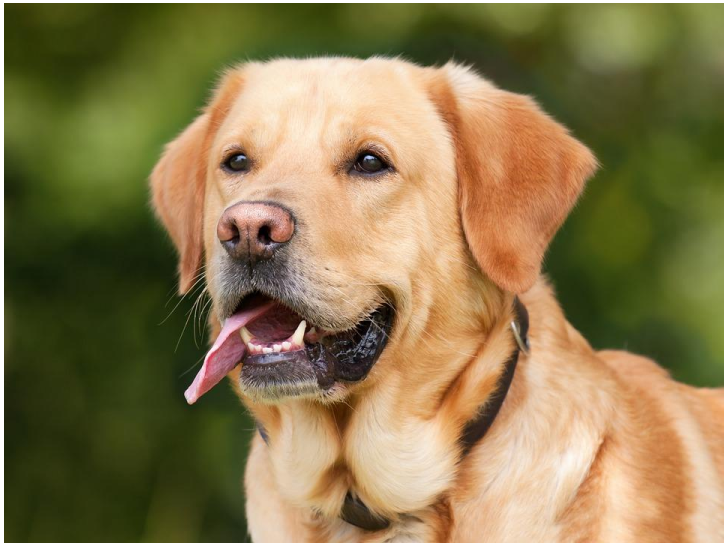
OUTPUT LAYER

ACTIVATED NEURONS

INPUT LAYER

DEEP *neural* NETWORK

Image Features



Google Cloud

A cat?

Google Cloud


Photo by: Arne Olav Gurvin Fredriksen -
https://www.instagram.com/ollafredriksen/

Google Cloud

Cloud Vision API

Mammal	99%
Vertebrate	99%
Dog Breed	95%
Dog	93%
Canidae	93%
Horse	85%
Stallion	83%
English Mastiff	76%

How would you classify this animal?

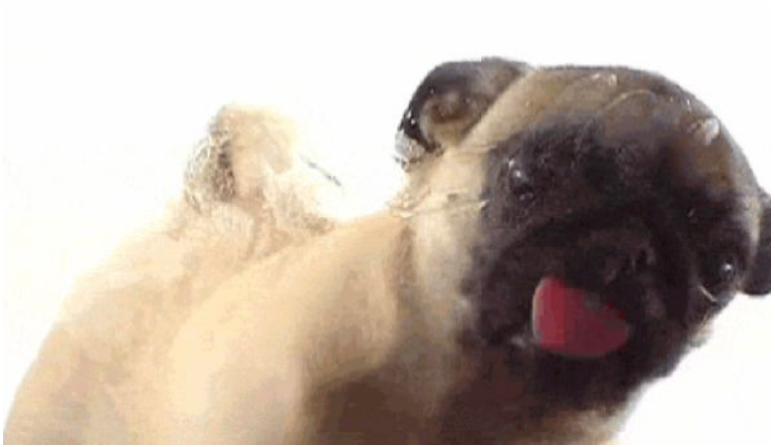
Photo by: Arne Olav Gurvin Fredriksen - https://www.instagram.com/ollafredriksen/

Behavioural Features

Barks, wiggles tail/lick, sleeps laying down, carnivore

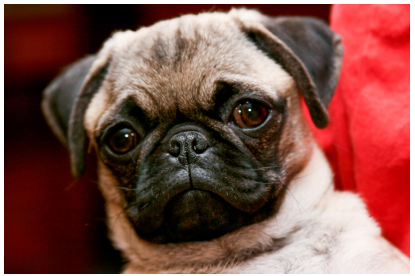
Neighs, bring head to owner, sleeps standing up, herbivorous

Behavioural Features



Barks, wiggles tail/lick, sleeps laying down, carnivore

Neighs, bring head to owner, sleeps standing up, herbivorous



EterPugBlue

+

DoubPulsar

=

WanaCry

Photo by: Arne Olav Gurvin Fredriksen - https://www.instagram.com/ollafredriksen/

Google Cloud

How does a malware behave?

Google Cloud

Malware Network Behaviour

Ransom

Port/Network Scanning

C&C Communication

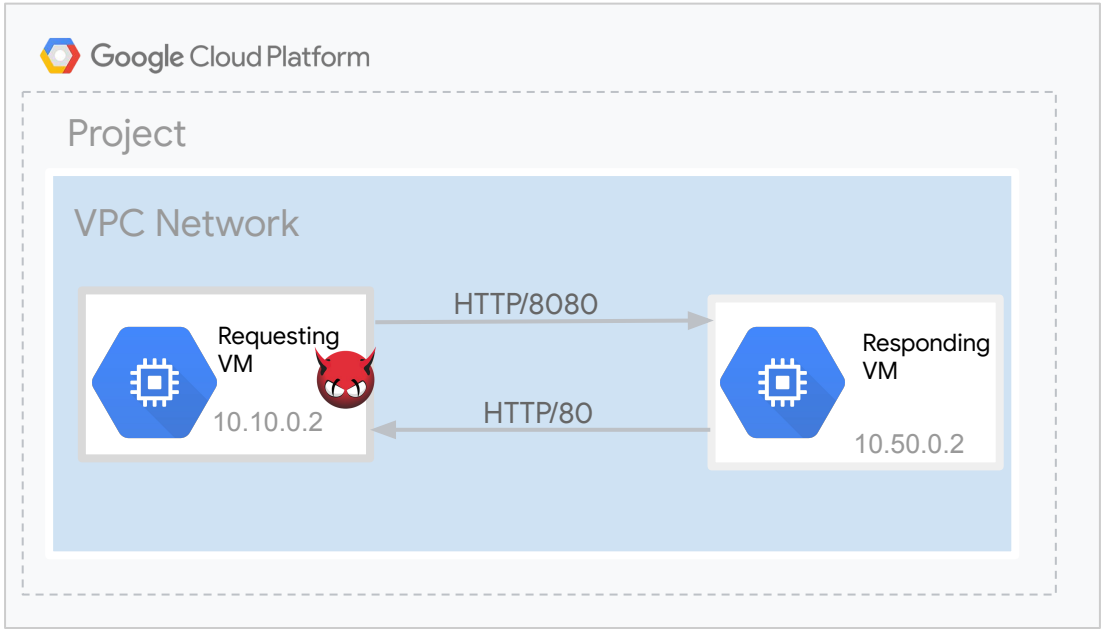
ClickFraud

DDoS

Email Spam

Google Cloud

How can we engineer features for malware detection?



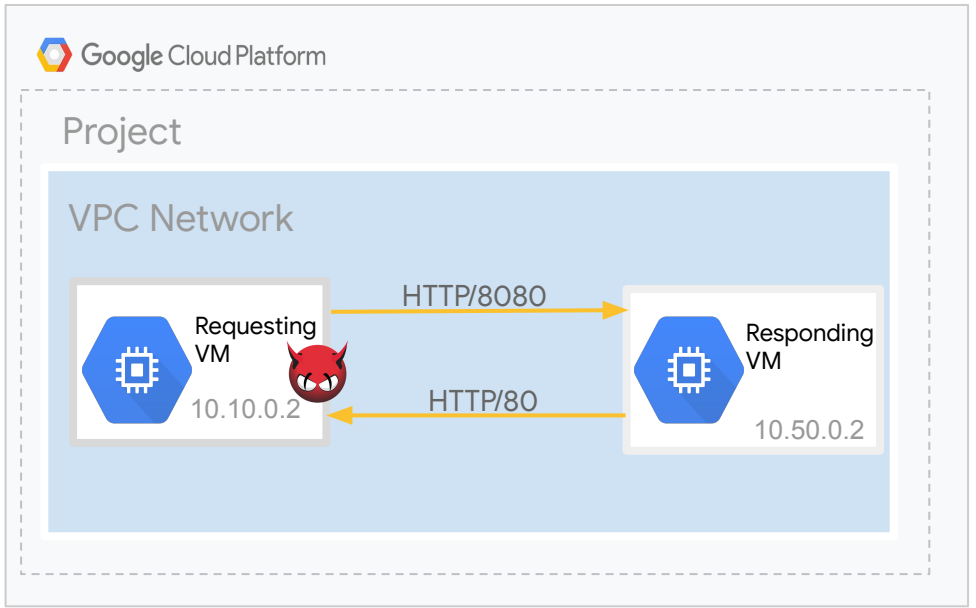
Google Cloud

Feature Engineering: Malware Network Sequence

LOG

10.10.0.2	1025	10.60.0.1	53	UDP	**DNS**	24	4
10.10.0.2	80	10.50.0.2	8080	TCP	**HTTP**	56	0
10.10.0.2	8080	10.50.0.2	80	TCP	**HTTP**	100	0
10.10.0.2	8080	10.50.0.2	80	TCP	**HTTP**	347	0
10.50.0.2	8080	10.10.0.2	80	TCP	**HTTP**	32	117

Google Cloud



Feature Engineering: Malware Network Sequence

Zeek Network Security Monitoring

10.10.0.2	1025	10.60.0.1	53	UDP	**DNS**	24	4
10.10.0.2	80	10.50.0.2	8080	TCP	**HTTP**	56	0
10.10.0.2	8080	10.50.0.2	80	TCP	**HTTP**	100	0
10.10.0.2	8080	10.50.0.2	80	TCP	**HTTP**	347	0
10.50.0.2	8080	10.10.0.2	80	TCP	**HTTP**	32	117

Google Cloud

Zeek Connection State Features

S0	Connection attempt seen, no reply.
S1	Connection established, not terminated.
SF	Normal establishment and termination.
REJ	Connection attempt rejected.
S2	Connection established and close attempt by originator seen (no reply from responder)
S3	Connection established and close attempt by responder seen (no reply from originator)
RST0	Connection established, originator aborted (sent a RST)
RSTR	Responder sent a RST
RSTOS0	Originator sent a SYN followed by a RST, but did not receive a SYN-ACK from the responder
RSTRH	Responder sent a SYN followed by a RST, but did not receive a SYN-ACK from the originator
SH	Originator sent a SYN followed by a FIN, we never saw a SYN ACK from the responder
SHR	Responder sent a SYN followed by a FIN, we never saw a SYN ACK from the Originator
OTH	No SYN seen, just midstream traffic

Feature Engineering: Malware Network Sequence

Zeek Network Security Monitoring

10.10.0.2	1025	10.60.0.1	53	UDP	**DNS**	24	4	→	SF
10.10.0.2	80	10.50.0.2	8080	TCP	**HTTP**	56	0	→	REJ
10.10.0.2	8080	10.50.0.2	80	TCP	**HTTP**	347	0	→	REJ
10.10.0.2	8080	10.50.0.2	80	TCP	**HTTP**	100	0	→	REJ
10.50.0.2	8080	10.10.0.2	80	TCP	**HTTP**	32	117	→	SF

Google Cloud

Zeek Connection State Features

S0	Connection attempt seen, no reply.
S1	Connection established, not terminated.
SF	Normal establishment and termination.
REJ	Connection attempt rejected.
S2	Connection established and close attempt by originator seen (no reply from responder)
S3	Connection established and close attempt by responder seen (no reply from originator)
RST0	Connection established, originator aborted (sent a RST)
RSTR	Responder sent a RST
RSTOS0	Originator sent a SYN followed by a RST, but did not receive a SYN-ACK from the responder
RSTRH	Responder sent a SYN followed by a RST, but did not receive a SYN-ACK from the originator
SH	Originator sent a SYN followed by a FIN, we never saw a SYN ACK from the responder
SHR	Responder sent a SYN followed by a FIN, we never saw a SYN ACK from the Originator
OTH	No SYN seen, just midstream traffic

Feature Engineering: Malware Network Sequence

Zeek Network Security Monitoring

S0 S1 REJ REJ REJ SF
SF SF SO OTH OTH SO
OTH SF SF SF SF SF
SO SO SO SF SF SF SO
S1 S1 SF SF SF SF SO
REJ REJ REJ REJ REJ
REJ REJ SO SO SO SO
SO SF SF SF SF SO SF

Google Cloud

Zeek Connection State Features

S0	Connection attempt seen, no reply.
S1	Connection established, not terminated.
SF	Normal establishment and termination.
REJ	Connection attempt rejected.
S2	Connection established and close attempt by originator seen (no reply from responder)
S3	Connection established and close attempt by responder seen (no reply from originator)
RST0	Connection established, originator aborted (sent a RST)
RSTR	Responder sent a RST
RSTOS0	Originator sent a SYN followed by a RST, but did not receive a SYN-ACK from the responder
RSTRH	Responder sent a SYN followed by a RST, but did not receive a SYN-ACK from the originator
SH	Originator sent a SYN followed by a FIN, we never saw a SYN ACK from the responder
SHR	Responder sent a SYN followed by a FIN, we never saw a SYN ACK from the Originator
OTH	No SYN seen, just midstream traffic

Feature Engineering: Malware Network Sequence

Network Flow Sequence

SOS1REJREJREJSFSFSFSOOTHOTHSOOTHSFSFSFSFSFSOSOSO

Text Sequence

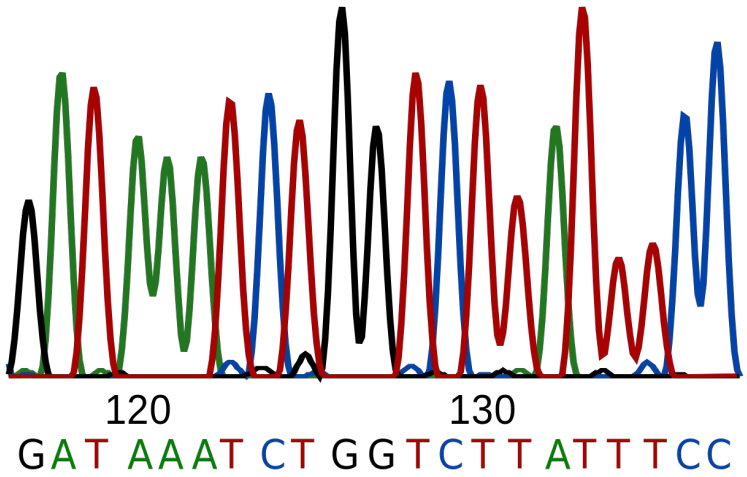
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

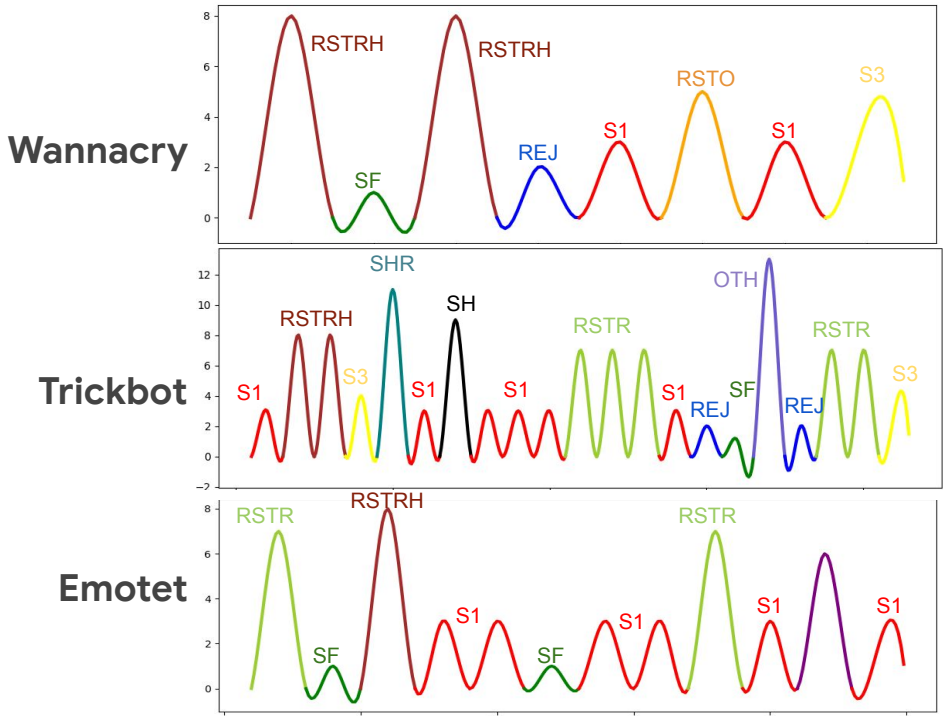
DNA Sequence

tccgagactcgatacagttgtgcagatgagctctggagacggggatcgtgtcgggtcgtttccgagactcgatacagttgtgcagatg

Google Cloud

DNA Sequencing

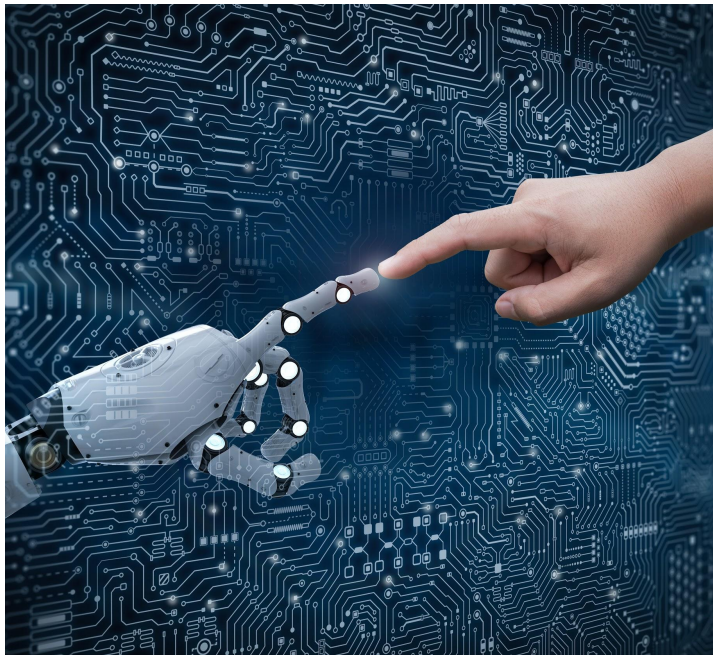




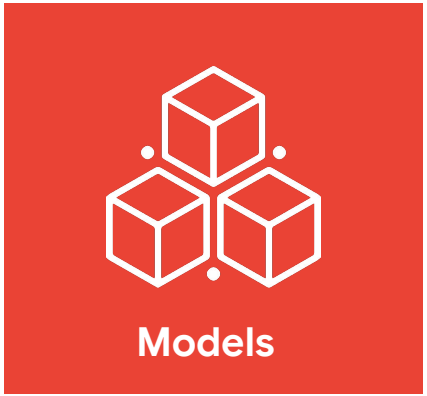
Google Cloud

Challenges: Feature Engineering

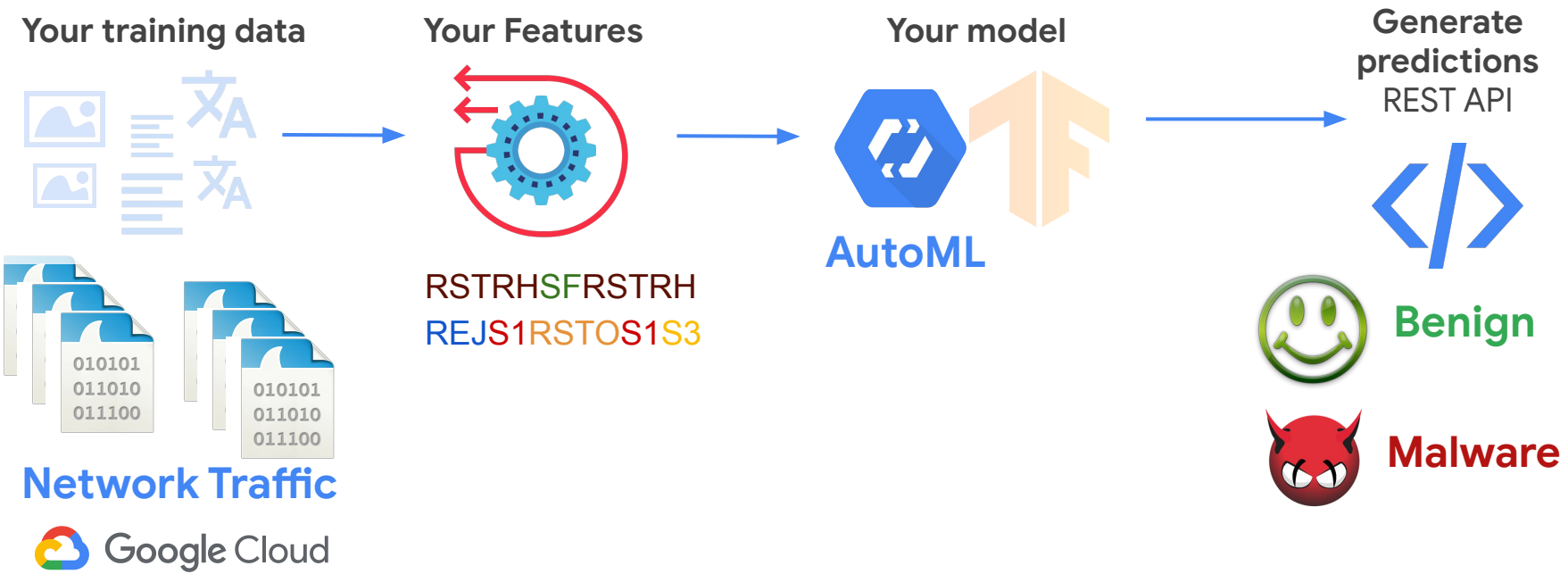
- The art and creativity in ML is in the feature engineering .
- Need expertise to engineer good features.
- Tedious and time-consuming.
- Adversaries change behaviour—Moving Target.



Machine Learning Building Blocks



Machine Learning Process



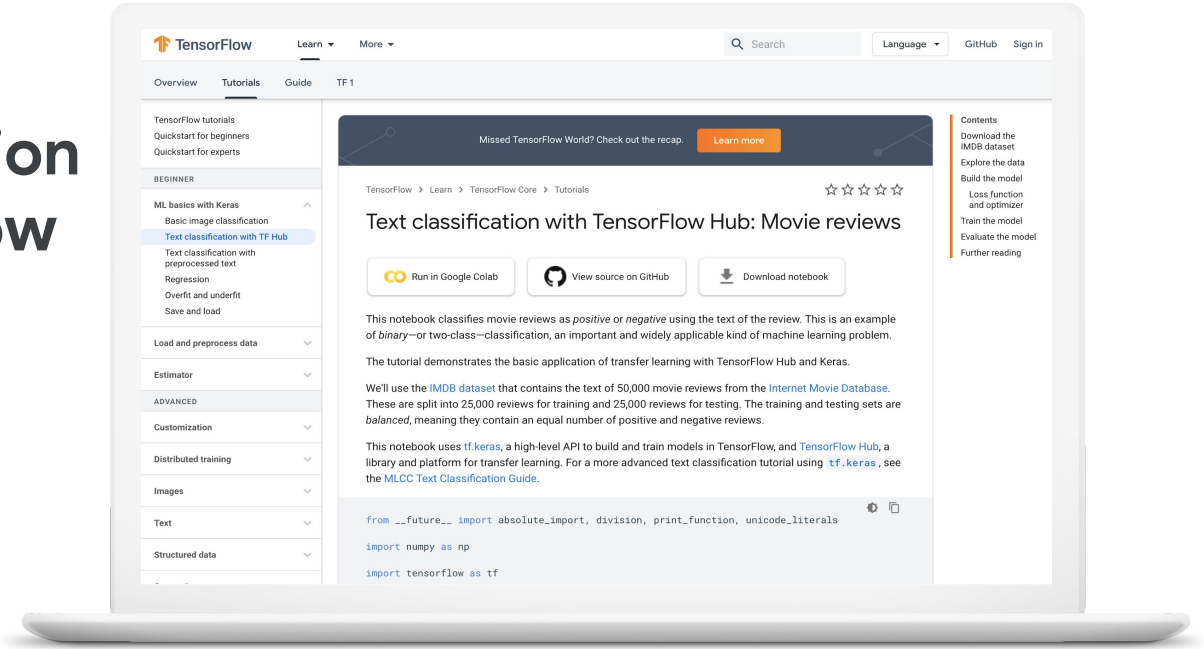
Demo

Google Cloud

Text Classification Using TensorFlow

Adapt existing sequence classification tutorials to security applications.

90%
F-measure

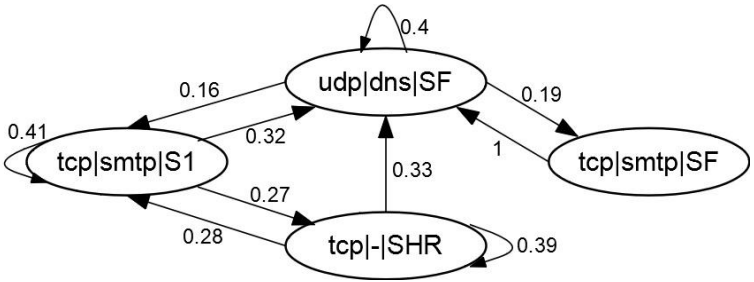


Google Cloud

Feature Engineering using Markov Chains

AsiaCCS 2020

Feature Engineering: Represent Malware Network behaviour as Markov Chain Model



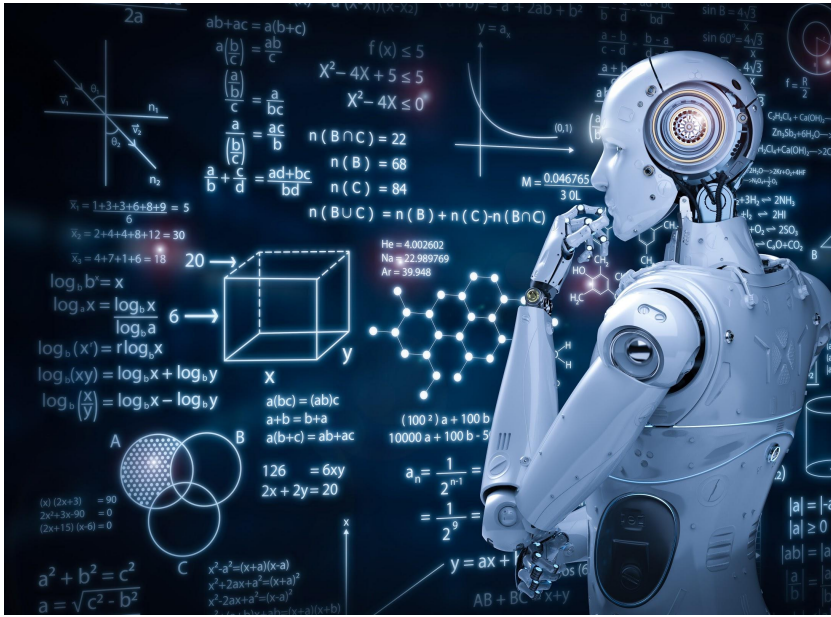
98%
F-measure
Known Malware

93%
F-measure
Unseen Malware

Google Cloud

Machine Learning Models - Myths

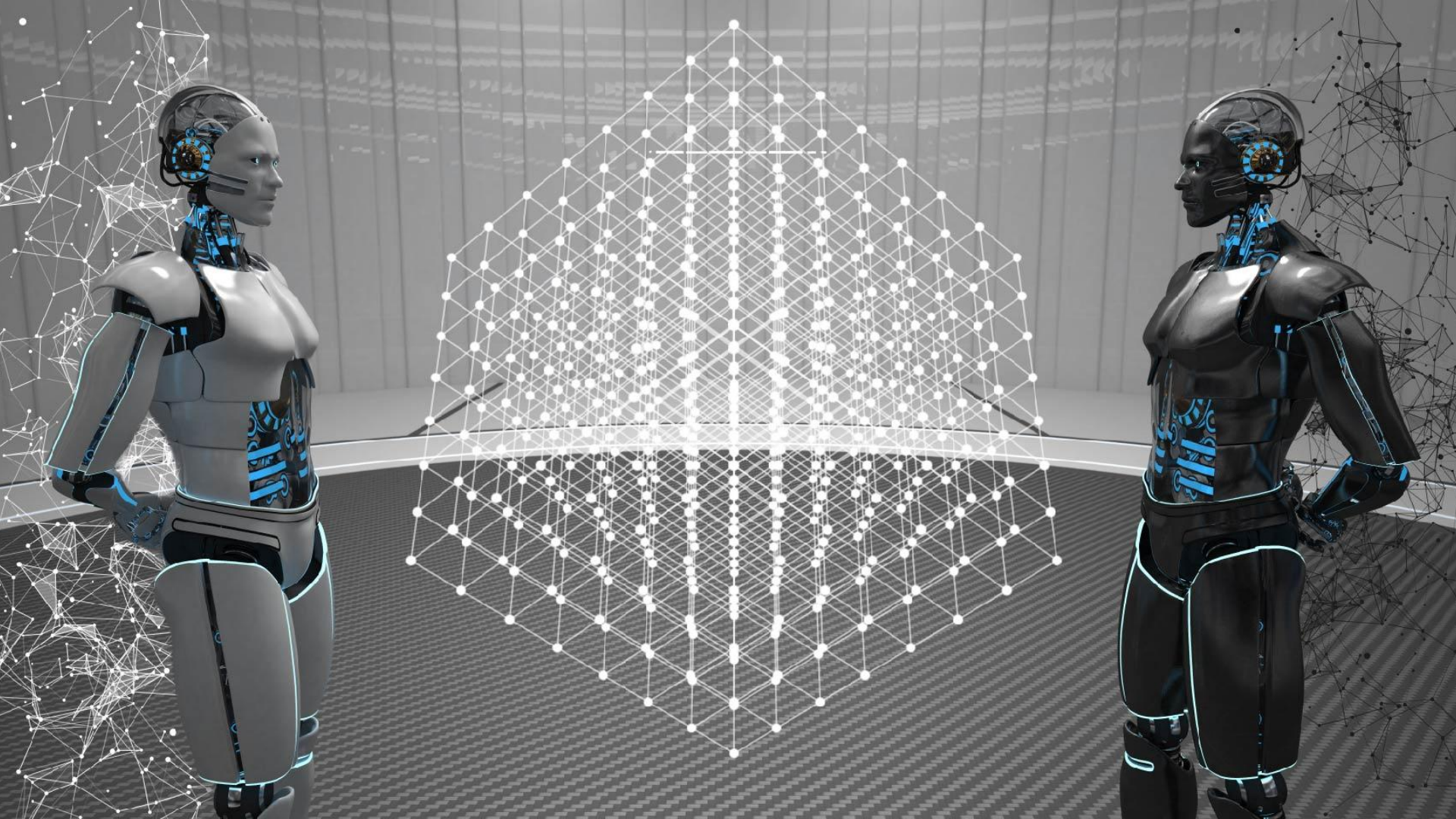
- Once the model has been trained and is deployed then I'm good to go!
- The accuracy of my model is **99%** so that's good.
- The most important thing is for the model to detect everything.
- The model learns on its own so there is not much humans have to do.



Google Cloud

More Challenges

Google Cloud



Main Takeaways

Build ML solutions for well-scoped problems with real data that provide actionable insights.

Use ML for problems where you have a large corpus of well labeled data to support modeling.

Leverage experienced domain experts for feature engineering.

Model should have a reduced cost of false negatives and false positives.

Verify your model.

Insights must be both accurate and actionable.

Adversaries and their tactics are moving targets.

Feedback is important.

Thank you

@BushraAlahmadi

Bushra.Alahmadi@cs.ox.ac.uk

Google Cloud