



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

Speaker: Bushra AlAhmadi

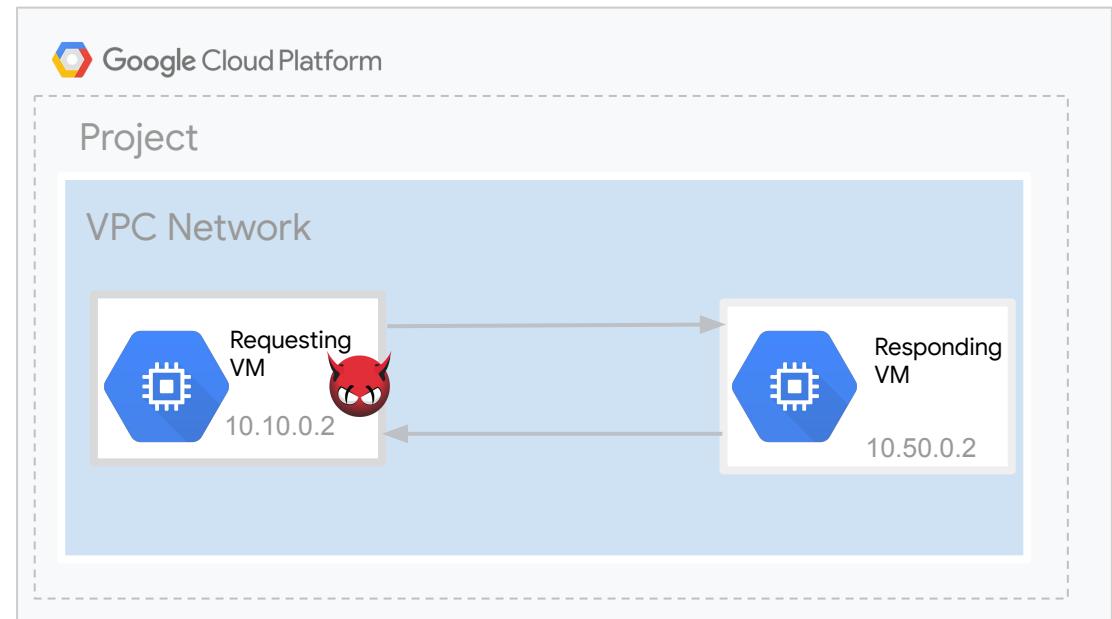
University of Oxford
@BushraAlahmadi

Google Cloud

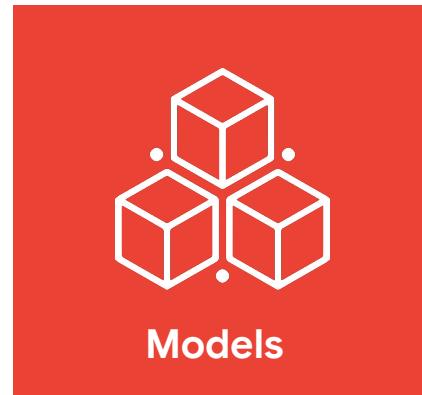
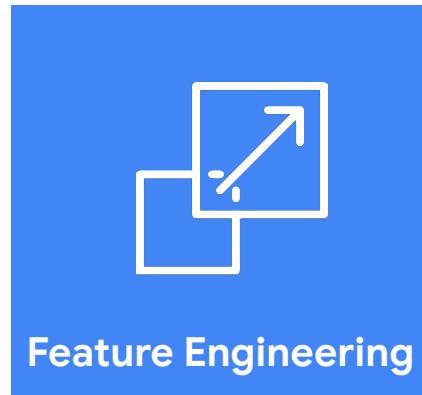




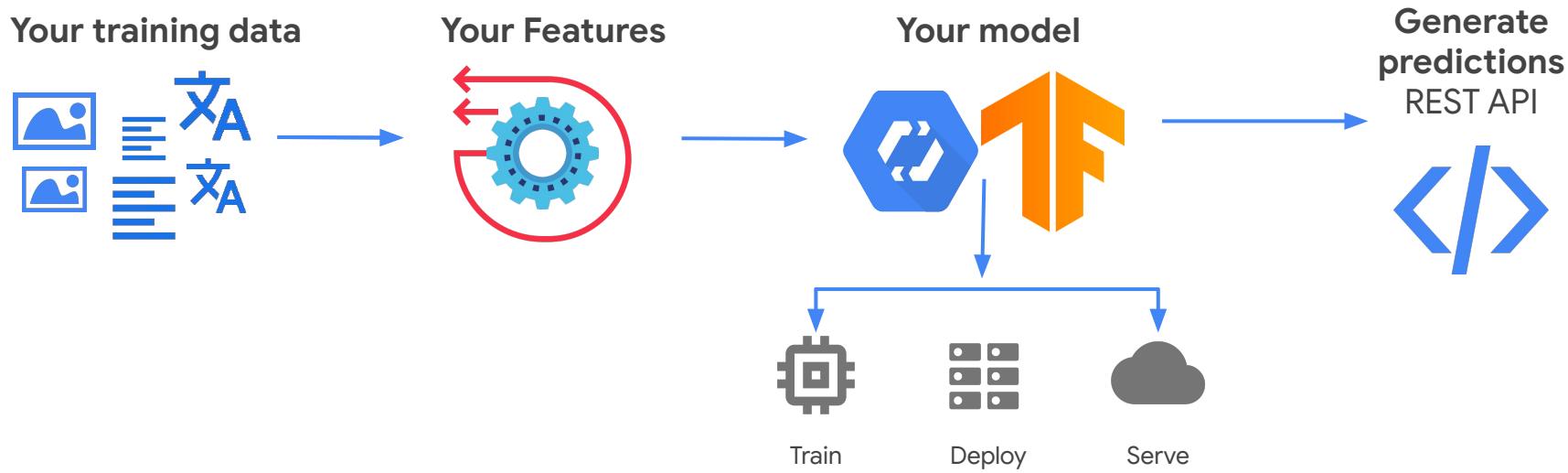
How can we detect malware on a VM?



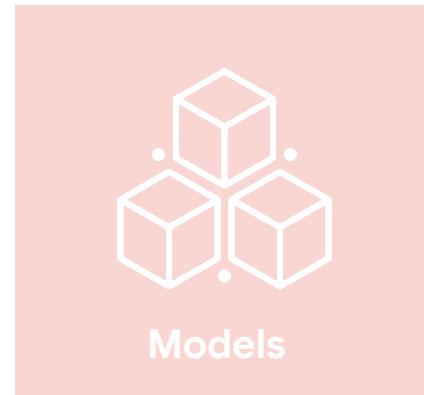
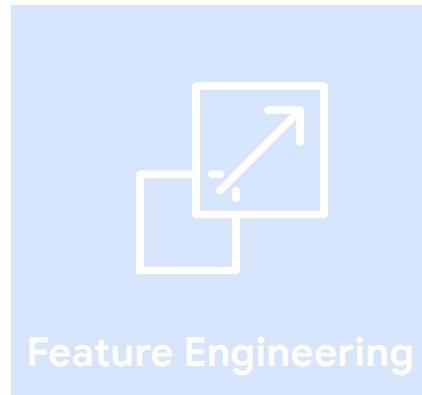
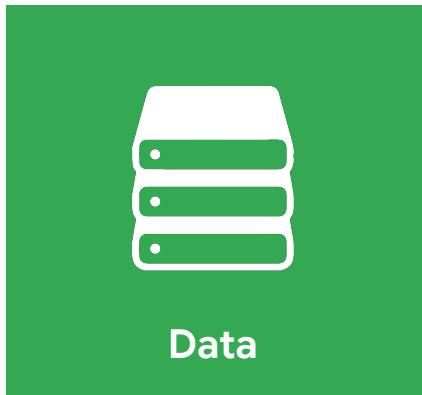
Machine Learning Building Blocks



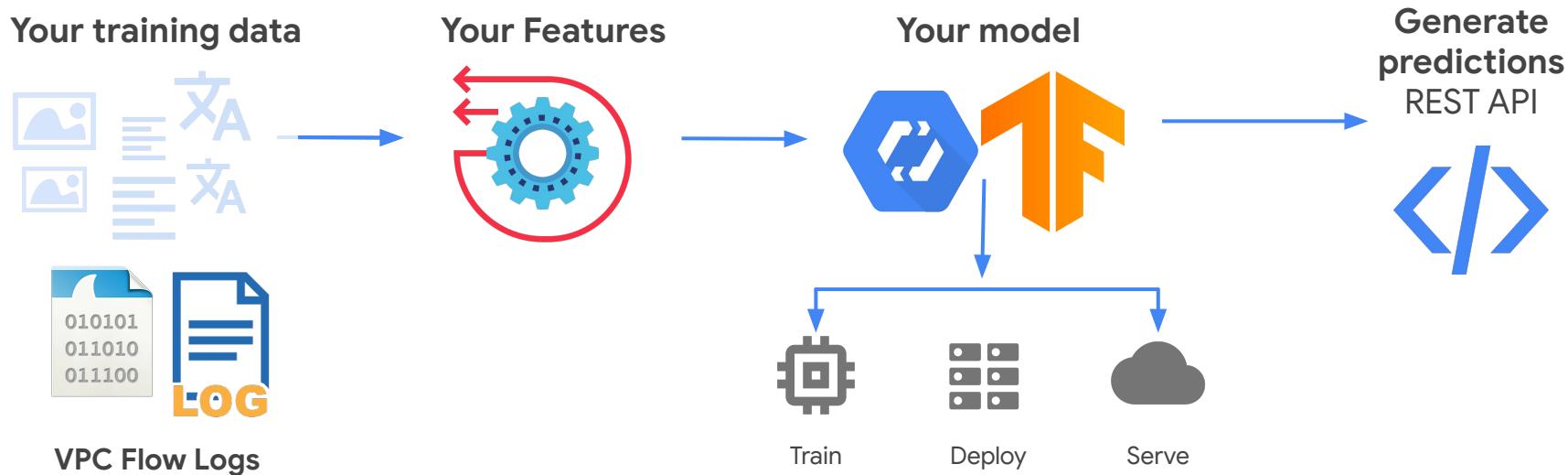
Machine Learning Process



Machine Learning Building Blocks



Machine Learning Process

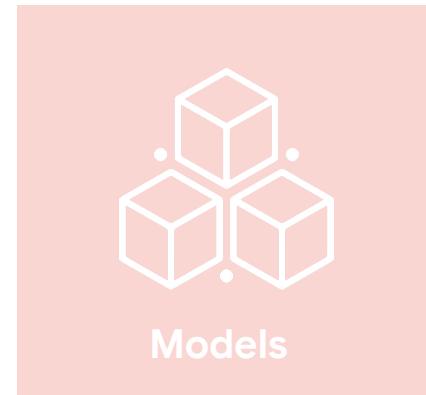
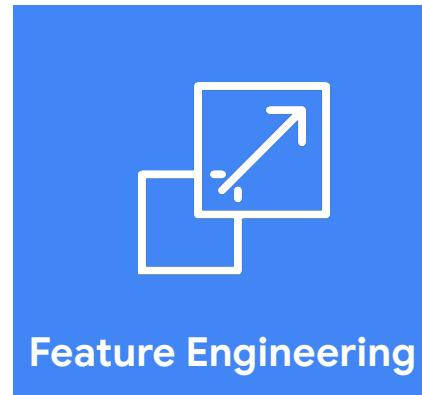


Data

- 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

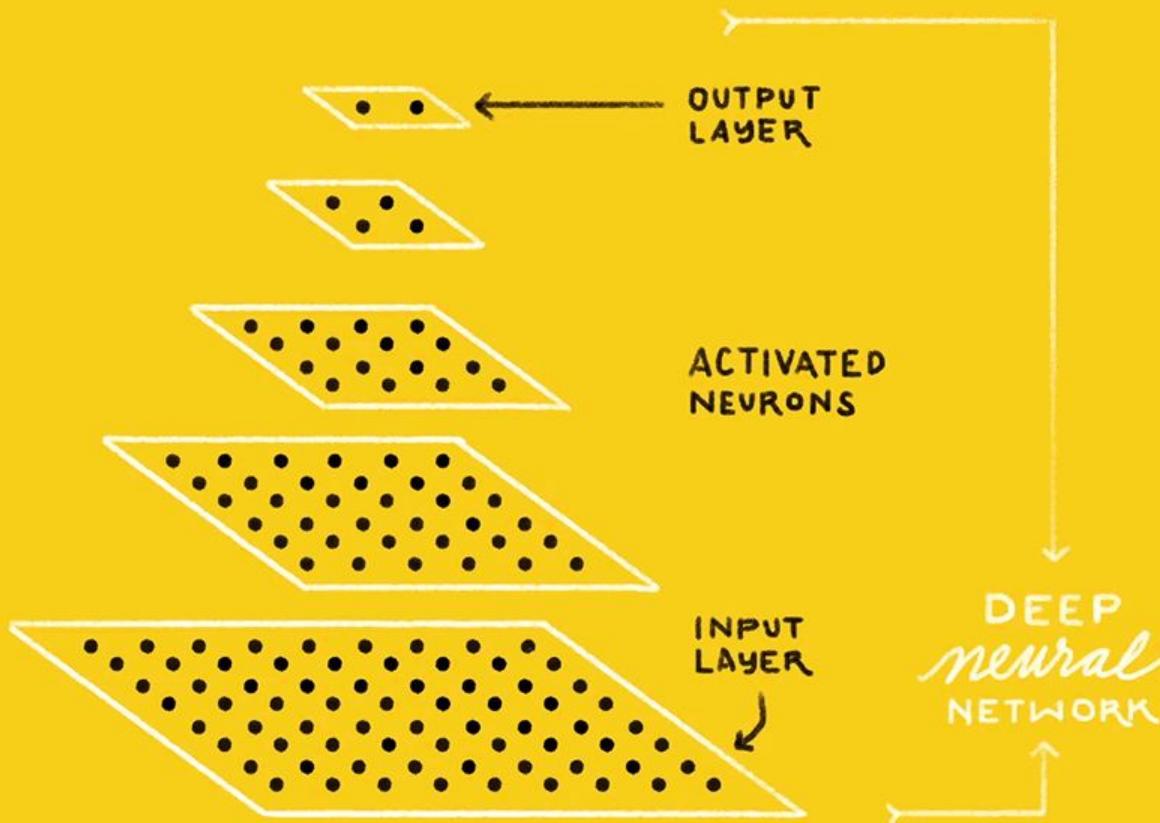


Image Features



A cat?

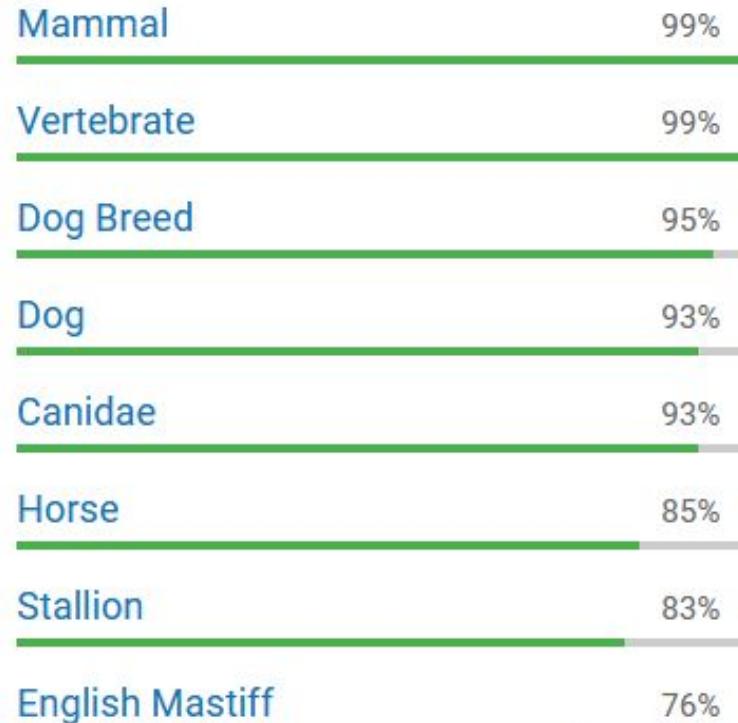




Photo by: Arne Olav Gurvin Fredriksen -
<https://www.instagram.com/ollafredriksen/>



Cloud Vision API



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



EtePugBlue



Digital Pulsar
Google Cloud



WapunCry



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

How does a malware behave?



Malware Network Behaviour



Ransom



Port/Network Scanning



C&C Communication



ClickFraud



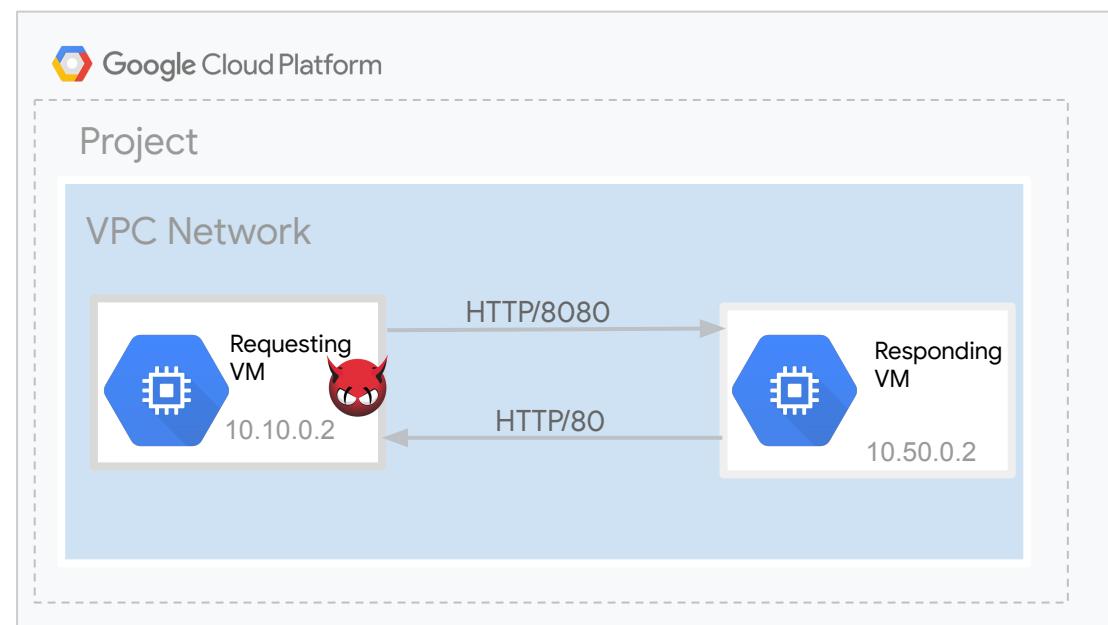
DDoS



Email Spam



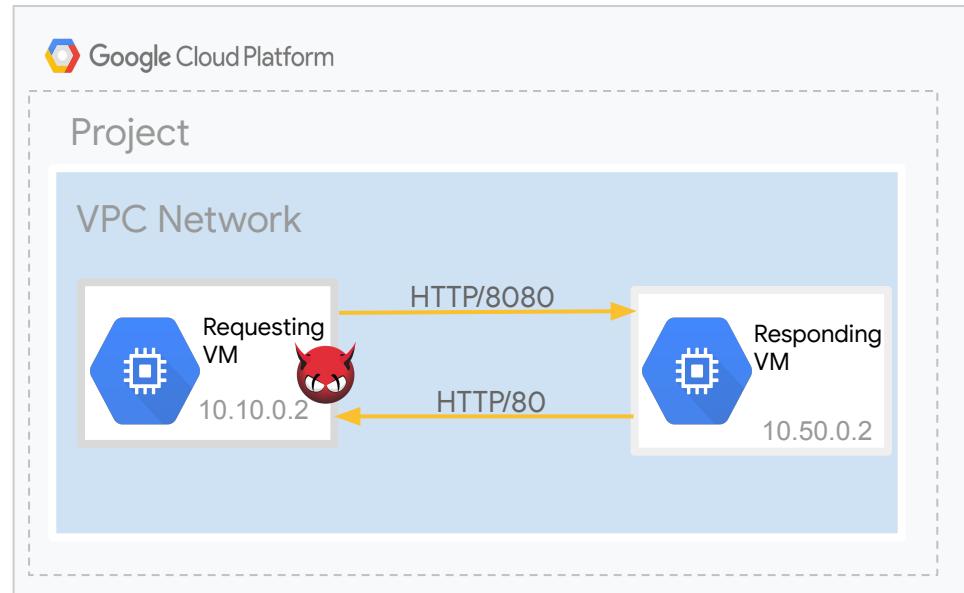
How can we engineer features for malware detection?



Feature Engineering: Malware Network Sequence



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	



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 O

10.10.0.2 8080 10.50.0.2 80 TCP **HTTP** 100 O

10.10.0.2 8080 10.50.0.2 80 TCP **HTTP** 347 O

10.50.0.2 8080 10.10.0.2 80 TCP **HTTP** 32 117

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

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

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

SOS1REJREJREJSFSFSFSOOOTHOTHSOOTHFSFSFSFSFSOSOSO

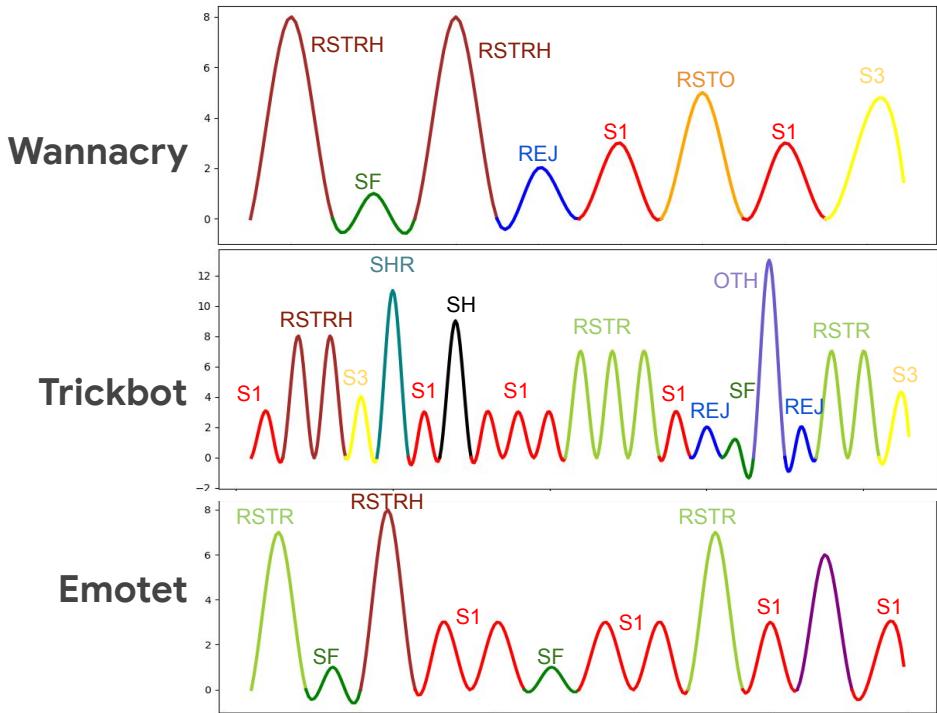
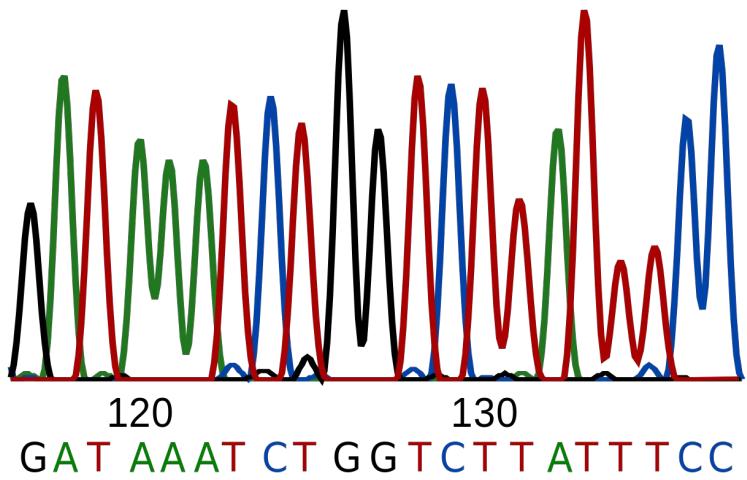
Text Sequence

THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG

DNA Sequence

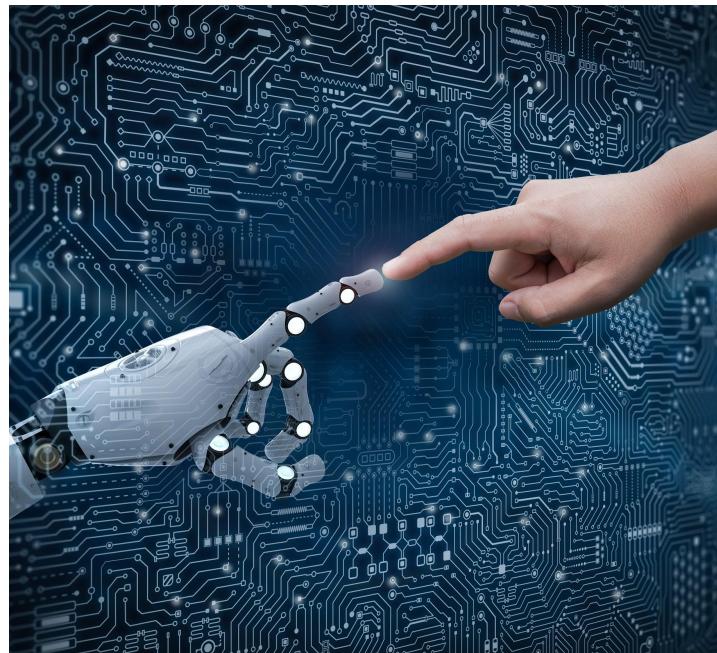
tccgagactcgatacagttgtgcagatgagctctggagaacggggatcggtgtcggttcgtttccgagactcgatacagttgtgcagatg

DNA Sequencing



Challenges: Feature Engineering

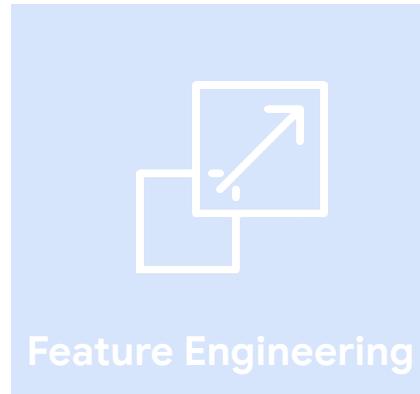
- The art and creativity in ML is in the feature engineering .
- Need expertise to engineer good features.
- Tedious and time-consuming.
- Adversaries change behaviour—Moving Target.



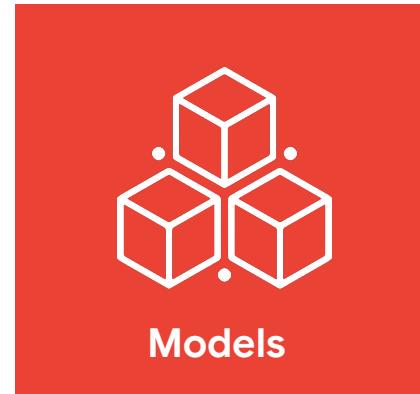
Machine Learning Building Blocks



Data

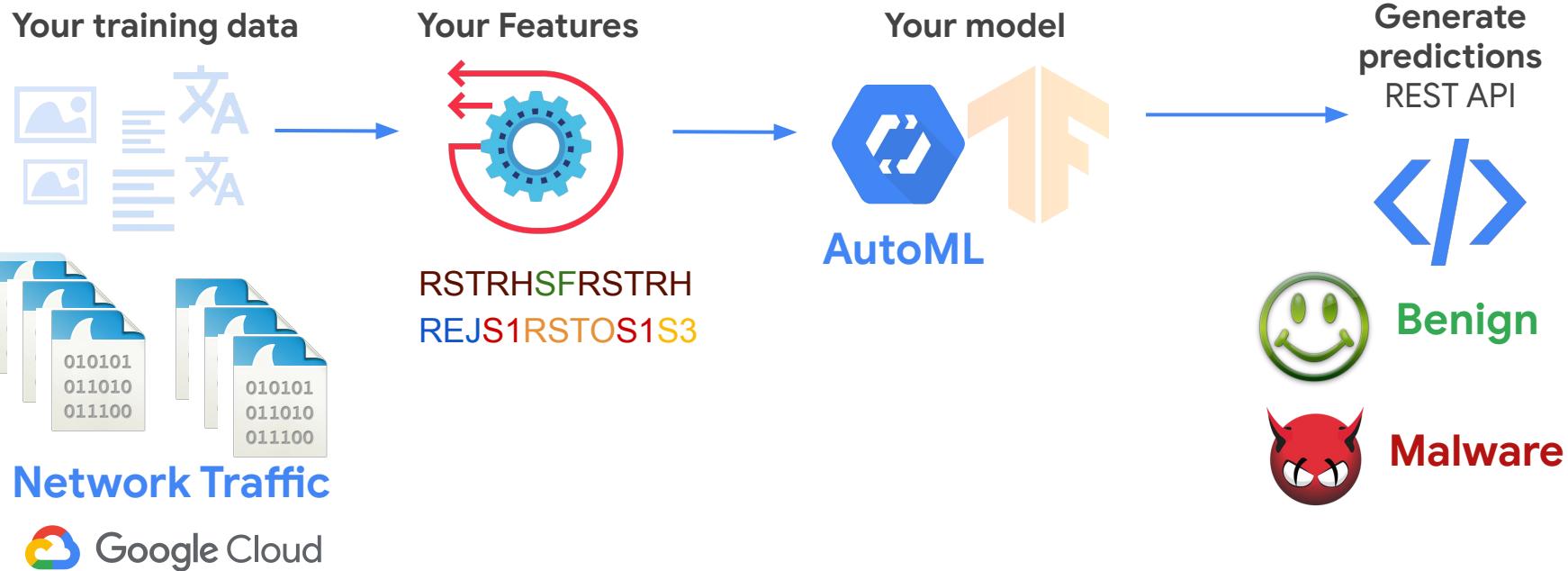


Feature Engineering



Models

Machine Learning Process



Demo

```
116  function(scope, element, attr, ngSwitchController) {  
117    var previousScope, element, attr, ngSwitchController;  
118    var attrChange = attr.ngSwitch || attr.on;  
119    var selectedTranscludes = [],  
120    selectedElements = [],  
121    previousElements = [],  
122    selectedScopes = [];  
123  
124    scope.$watch(attrExpr, function ngSwitchWatchAction(value) {  
125      var i, ii;  
126      for (i = 0, ii = previousElements.length; i < ii; ++i) {  
127        previousElements[i].remove();  
128      }  
129      previousElements.length = 0;  
130  
131      for (ii = 0, ii = selectedScopes.length; i < ii; ++i) {  
132        var selected = selectedElements[i];  
133        selectedScopes[i].$destroy();  
134        previousElements[i] = selected;  
135        $animate.leave(selected, function() {  
136          previousElements.splice(i, 1);  
137        });  
138      }  
139  
140      selectedElements.length = 0;  
141      selectedScopes.length = 0;  
142  
143      if ((selectedTranscludes = ngSwitchController.cases['!'] + value)) {  
144        scope.$eval(attr.change);  
145        forEach(selectedTranscludes, function(selectedTransclude) {  
146          var selectedScope = scope.$new();  
147          selectedScopes.push(selectedScope);  
148        });  
149      }  
150    });  
151  }  
152  
```

Text Classification Using TensorFlow

Adapt existing sequence classification tutorials to security applications.

90%
F-measure

The screenshot shows the TensorFlow website's 'Tutorials' section. The left sidebar has categories like Overview, Tutorials (selected), Guide, and TF 1. Under 'Tutorials', there are sections for TensorFlow tutorials, Beginner, ML basics with Keras, Estimator, ADVANCED, Customization, Distributed training, Images, Text, and Structured data. The 'Text classification with TensorFlow Hub: Movie reviews' notebook is selected under 'ML basics with Keras'. The main content area shows the title 'Text classification with TensorFlow Hub: Movie reviews', navigation links ('Run in Google Colab', 'View source on GitHub', 'Download notebook'), a brief description of the task, and a snippet of the Python code at the bottom:

```
from __future__ import absolute_import, division, print_function, unicode_literals
import numpy as np
import tensorflow as tf
```



Feature Engineering using Markov Chains

Feature Engineering: Represent
Malware Network behaviour as
Markov Chain Model

98%

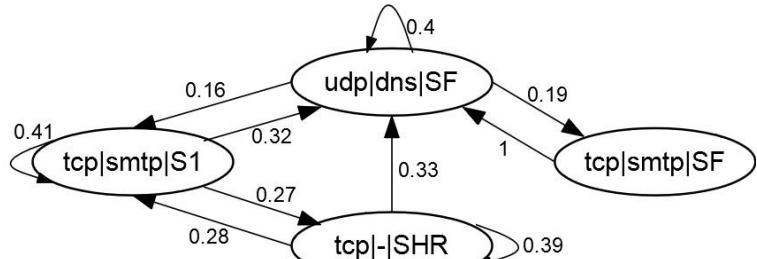
F-measure

Known Malware

93%

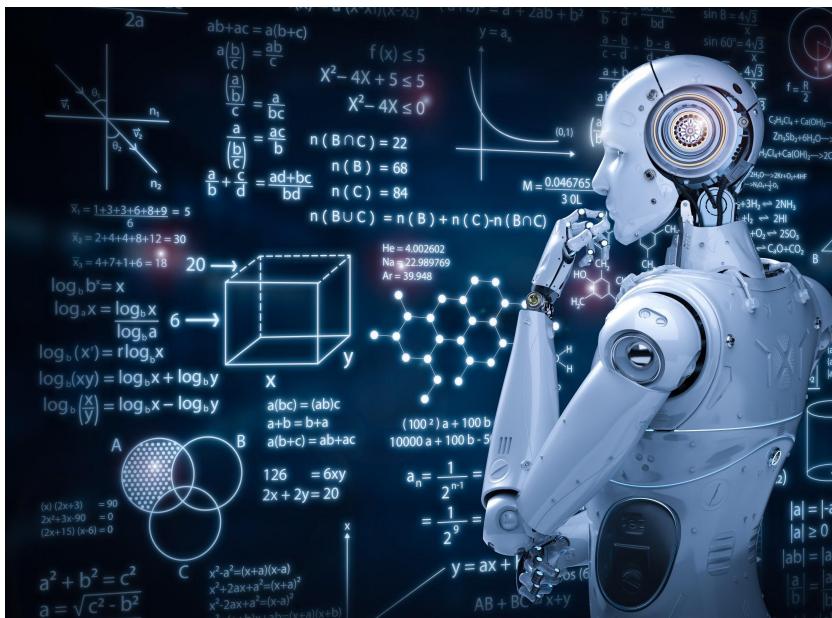
F-measure

Unseen Malware



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.

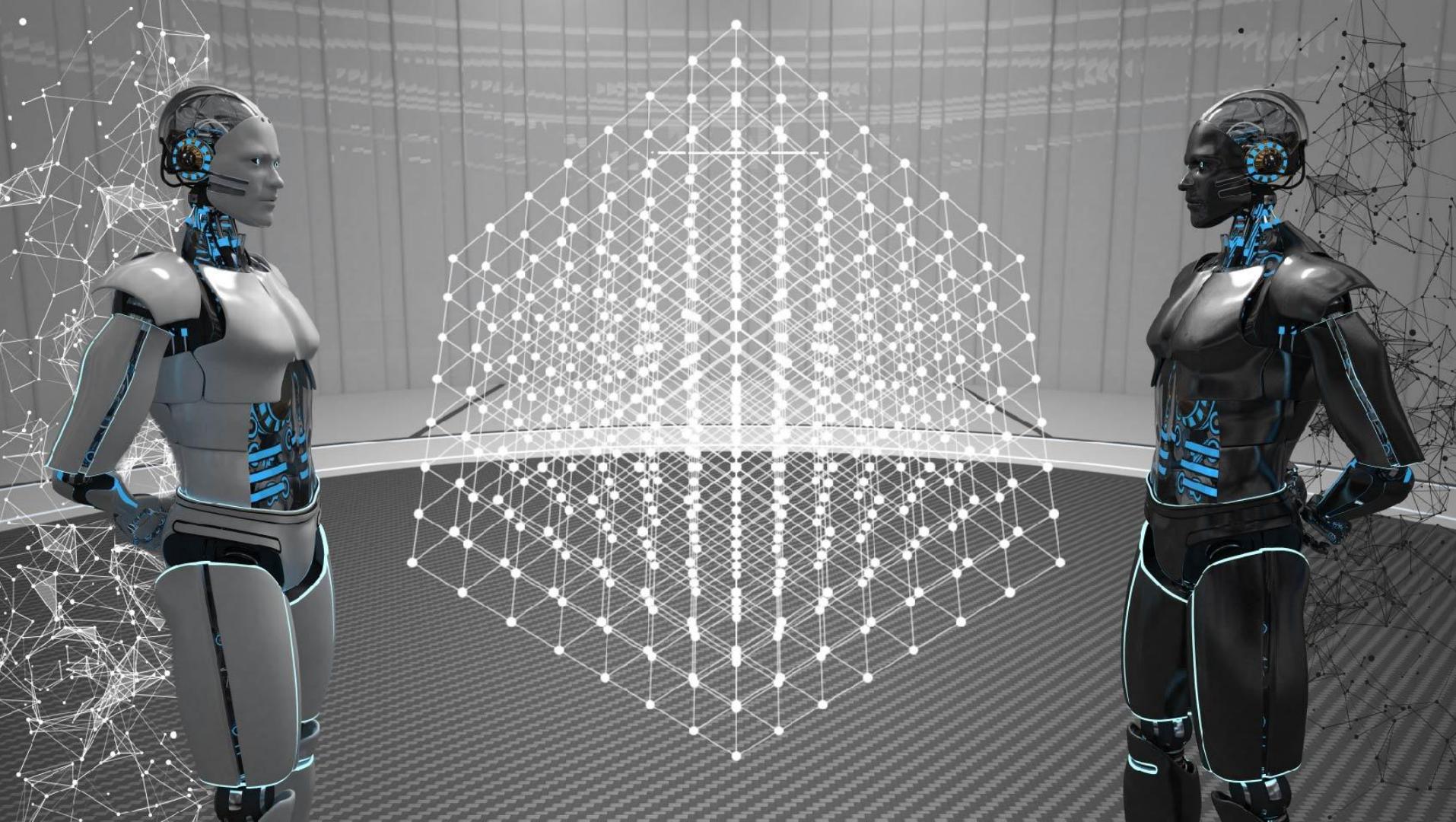




More Challenges

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