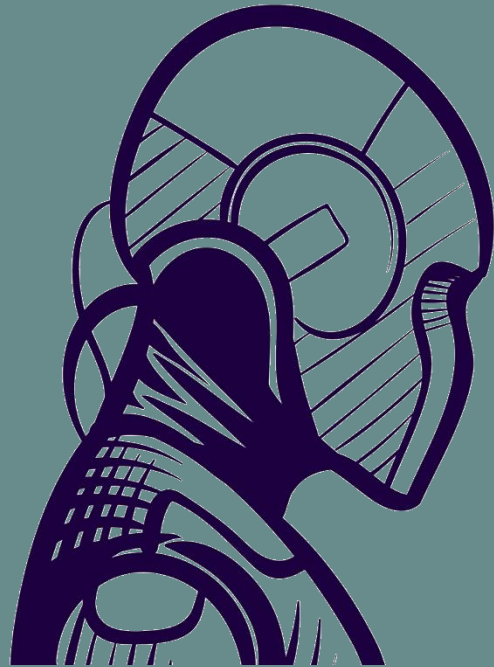


The machine world



The human world



ORACLE

Challenges in adopting Machine Learning for Cybersecurity

Desislava Dimitrova

Matteo Casserini

Oracle Labs Zurich



PREVENTION

Identity & access control
Vulnerability management
Threat Intelligence

MITIGATION

Data forensics
Suggest an action plan
Automated corrective actions

ML

Log analysis
Real-time analysis
Anomaly detection and alerting

Extract insights
Build new threat profiles

DETECTION

REFLECTION

3 challenges

The Method

The Data

The Adoption

The method challenge



The first key to success is understanding the use case

Use case:

Alert prioritization to decrease alert fatigue

Requirements:

Performance optimization vs secure operation



The first key to success is understanding the use case

Use case:

SQL log analysis to detect abnormal queries

Requirements:

Anomaly detection vs Query classification



Road Bike



Cruiser



Fixed Gear



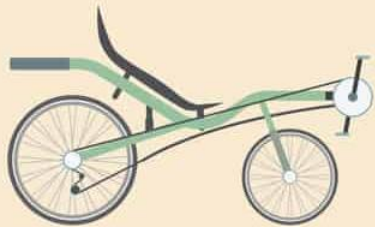
Mountain Bike



BMX



Touring Bike



Recumbent bike



folding bike



Utility Bike

Finding the proper means (method) to solve a problem





Less is more:
finding the solution that
gets the job done

Accuracy

+

Latency

+

Run-time performance

Minimal workable solution

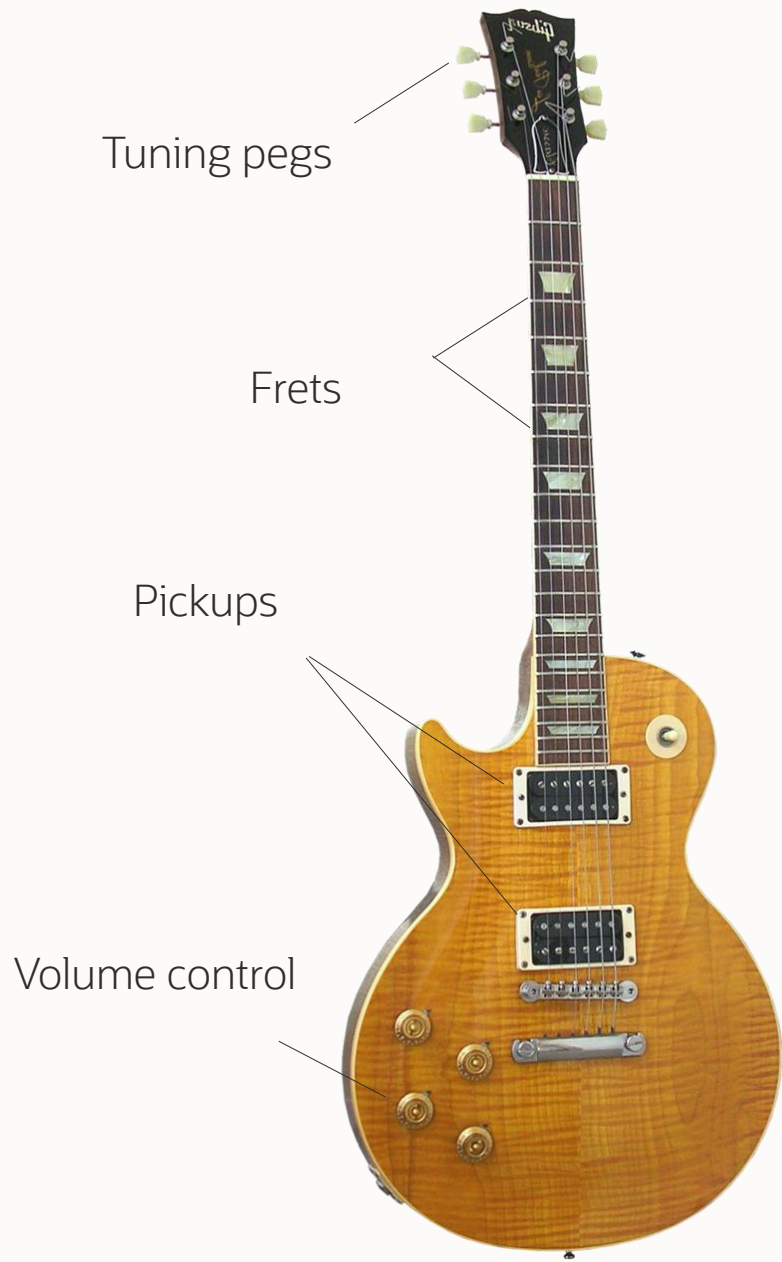


The data challenge



You Can't Always Get
What You Want





Understanding input data
is not always trivial

The quest for data labelling

We will rock you, Rock


Verse
Moderately, in 2
N.C.(Em)
mf
1. Bud - dy, you're a boy, make a big noise play - in' in the street, gon - na be a big
2., 3. See additional lyrics



The image shows the musical notation for the verse of 'We Will Rock You'. It includes a vocal line in treble clef with lyrics and a guitar tablature below it. The tempo is 'Moderately, in 2' and the key signature is one flat (Em). The guitar part consists of a simple bass line with triplets of eighth notes.

Fly me to the moon, Jazz

♩ = 80



The image shows the musical notation for 'Fly Me to the Moon'. It features a complex jazz guitar line in treble clef with many accidentals and a corresponding guitar tablature below it. The tempo is marked as ♩ = 80.

Hallelujah, Classic

♩ = 60
INTRO
G Em G Em



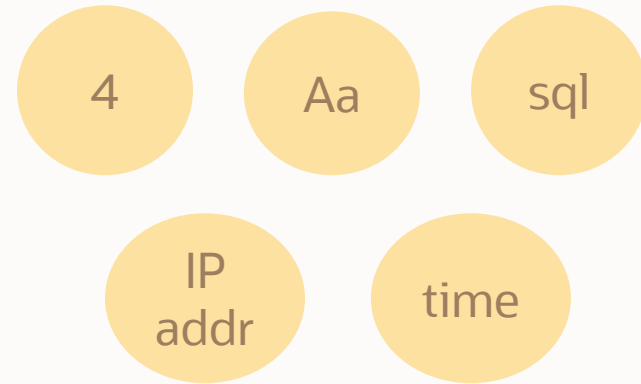
The image shows the musical notation for the intro of 'Hallelujah'. It includes a guitar line in treble clef with a steady eighth-note accompaniment and a guitar tablature below it. The tempo is marked as ♩ = 60. The key signature is one flat (Em). The guitar part features a simple bass line with eighth notes.





System logs are a motley crew for encoding

System logs



The adoption challenge



“It’s just an educated guess.”

“Why should I trust an algorithm that cannot explain its result?”

“How does my role change?”

Accept

Use



sustain

deploy

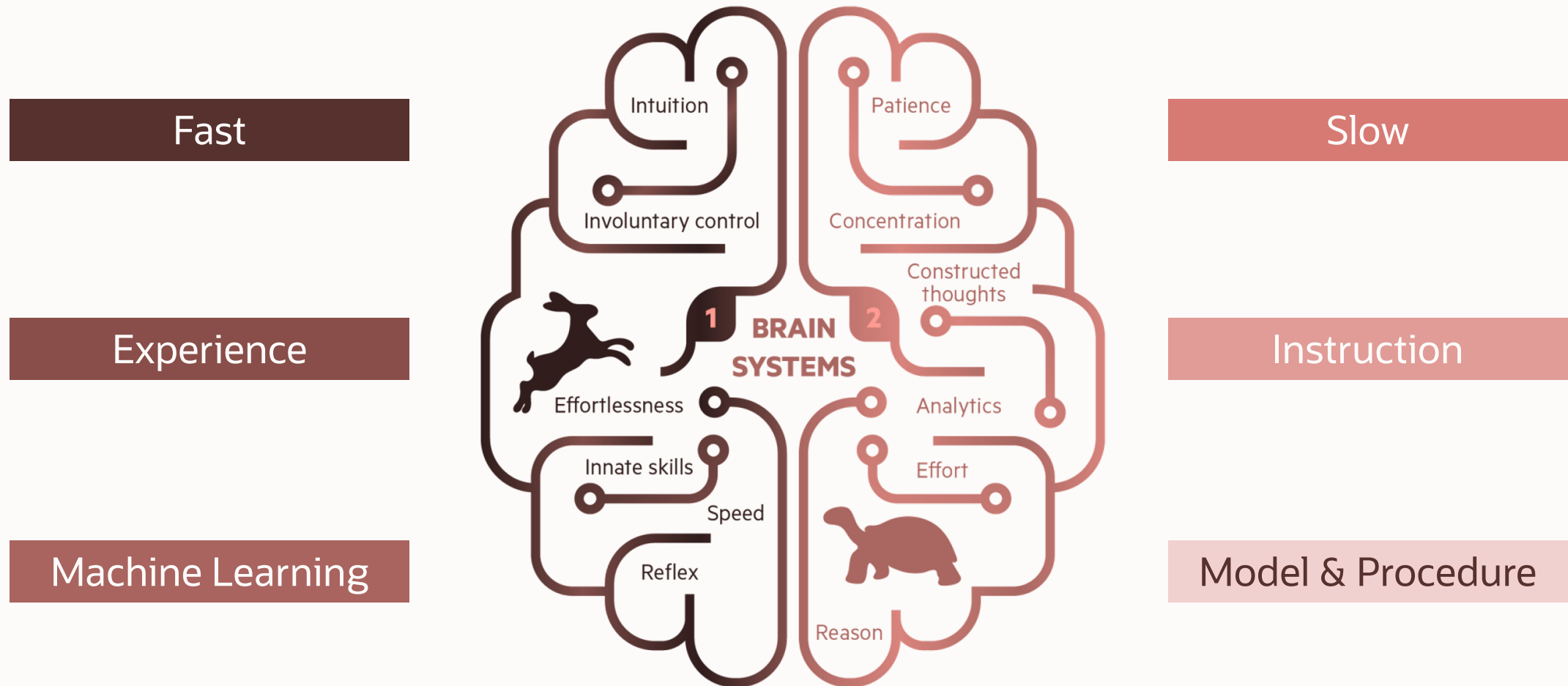
trust

value

relate



How do humans learn? A tale of two systems





What's in it for ME?

What are your PAIN POINTS?

Demonstrate VALUE.

Highlight LIMITATIONS.



What's in it for ME?

What are your PAIN POINTS?

Demonstrate VALUE.

Highlight LIMITATIONS.

How does my role CHANGE?

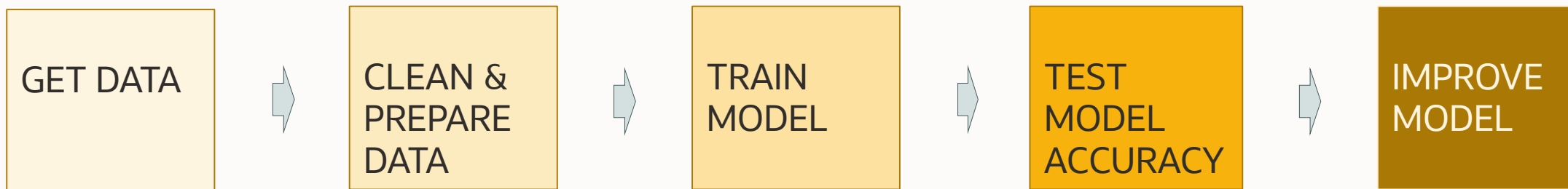
We need your EXPERTISE.

Allow EXPLORATION.

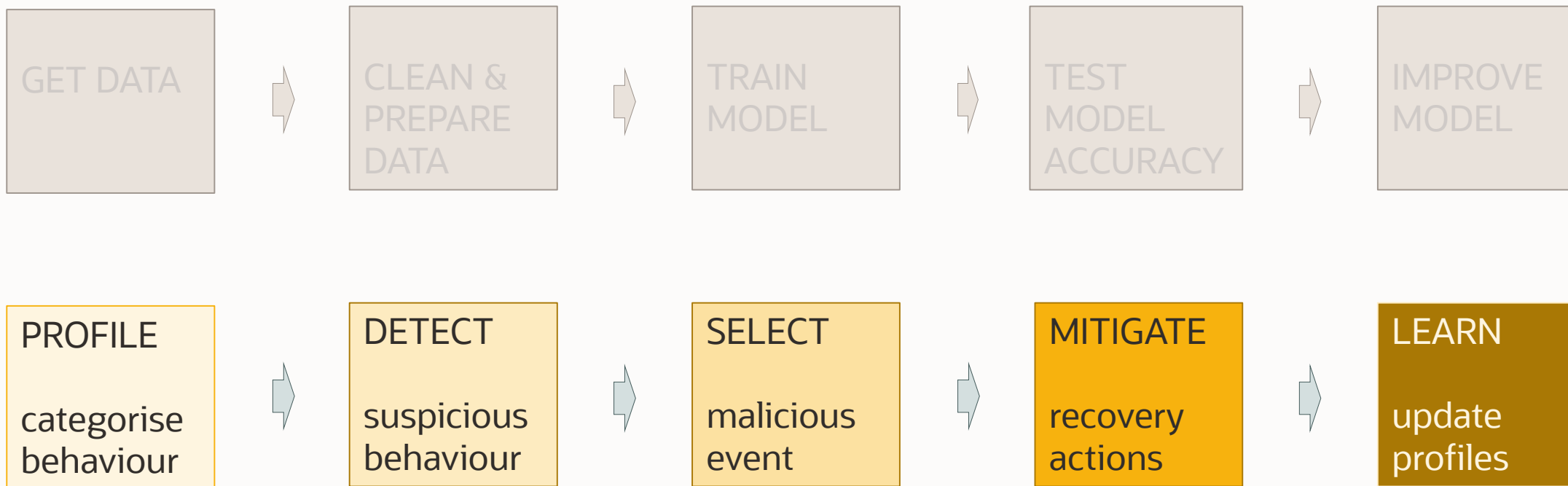


trust me
Explainable AI

How to deploy ML?



How to deploy ML **in production?**



What is the cost of maintenance?

